

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		班级		学号		姓名	
完成日期： 2017 年 月 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】

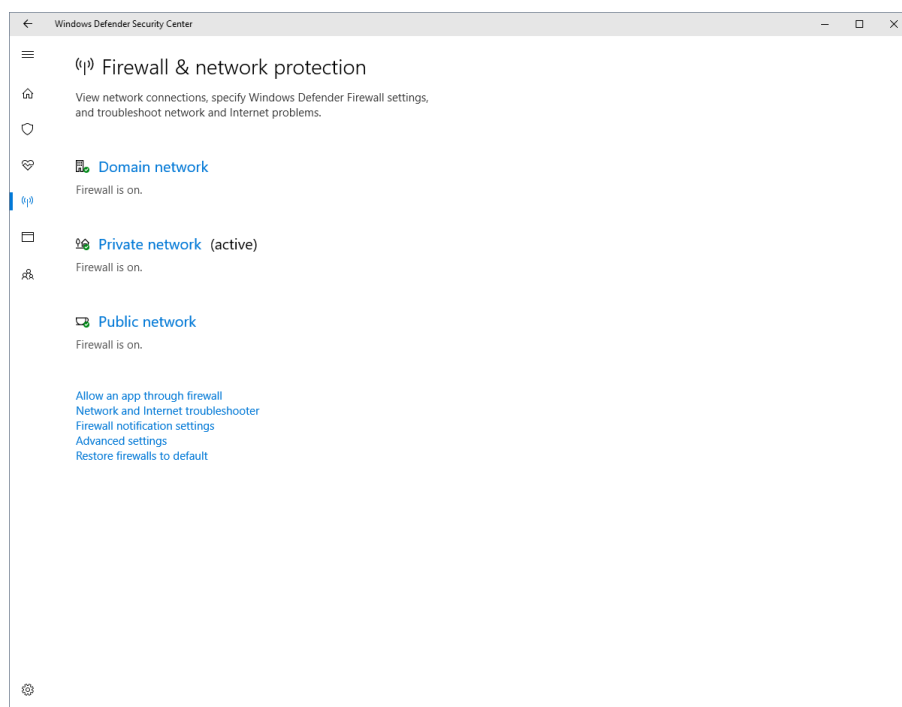
所有进出网络的信息都必须通过防火墙，所以防火墙是一个安全策略的检查站，是设置在被保护网络和外部网络之间的一道屏障。防火墙对流经它的网络通信进行扫描，防止发生不可预测的、潜在破坏性的侵入。防火墙不但可以关闭不使用的端口，它还能禁止特定端口的流出通信，封锁特洛伊木马。另外，防火墙还可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

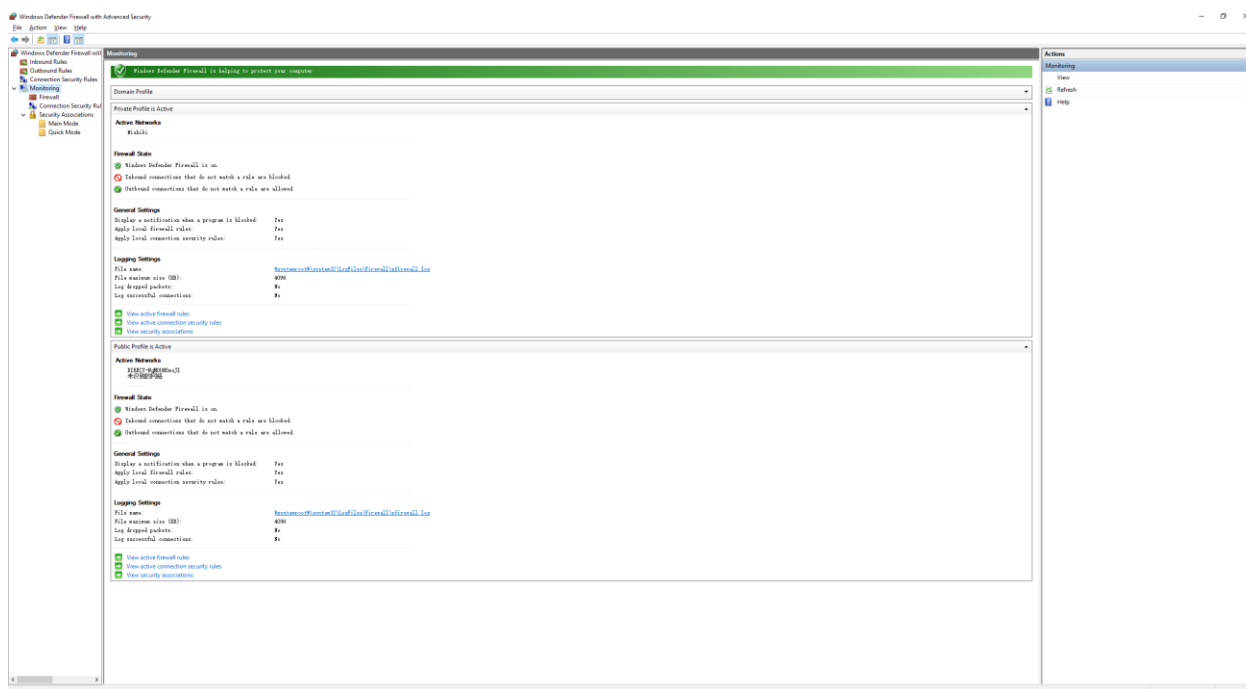
【实验要求】

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）。





功能描述

具有高级安全性的 Windows Defender 防火墙是分层安全模型的重要组成部分。通过为设备提供基于主机的双向网络流量过滤，Windows Defender 防火墙可阻止未经授权的网络流量流入或流出本地设备。Windows Defender 防火墙还可以与网络感知协同工作，以便可以应用与设备所连接的网络类型相适应的安全设置。Windows Defender 防火墙和 Internet 协议安全 (IPsec) 配置设置已集成到名为 Windows Defender 防火墙的单个 Microsoft 管理控制台 (MMC) 中，因此 Windows Defender 防火墙也是网络隔离策略的重要组成部分。

实际应用

为帮助解决组织的网络安全难题，Windows Defender Firewall 提供了以下优势：

1. 降低网络安全威胁的风险。Windows Defender 防火墙减少了设备的攻击面，为防御深度模型提供了额外的层。减少设备的攻击面增加了可管理性，并降低了成功攻击的可能性。
 2. 保护敏感数据和知识产权。通过与 IPsec 集成，Windows Defender 防火墙提供了一种简单的方法来执行经过身份验证的端到端网络通信。它提供对可信任网络资源的可扩展的分层访问，有助于强制执行数据的完整性，并可选地帮助保护数据的机密性。
 3. 扩大现有投资的价值。由于 Windows Defender 防火墙是操作系统附带的基于主机的防火墙，因此不需要额外的硬件或软件。Windows Defender 防火墙还旨在通过文档化的应用程序编程接口 (API) 补充现有的非 Microsoft 网络安全解决方案。
- (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。

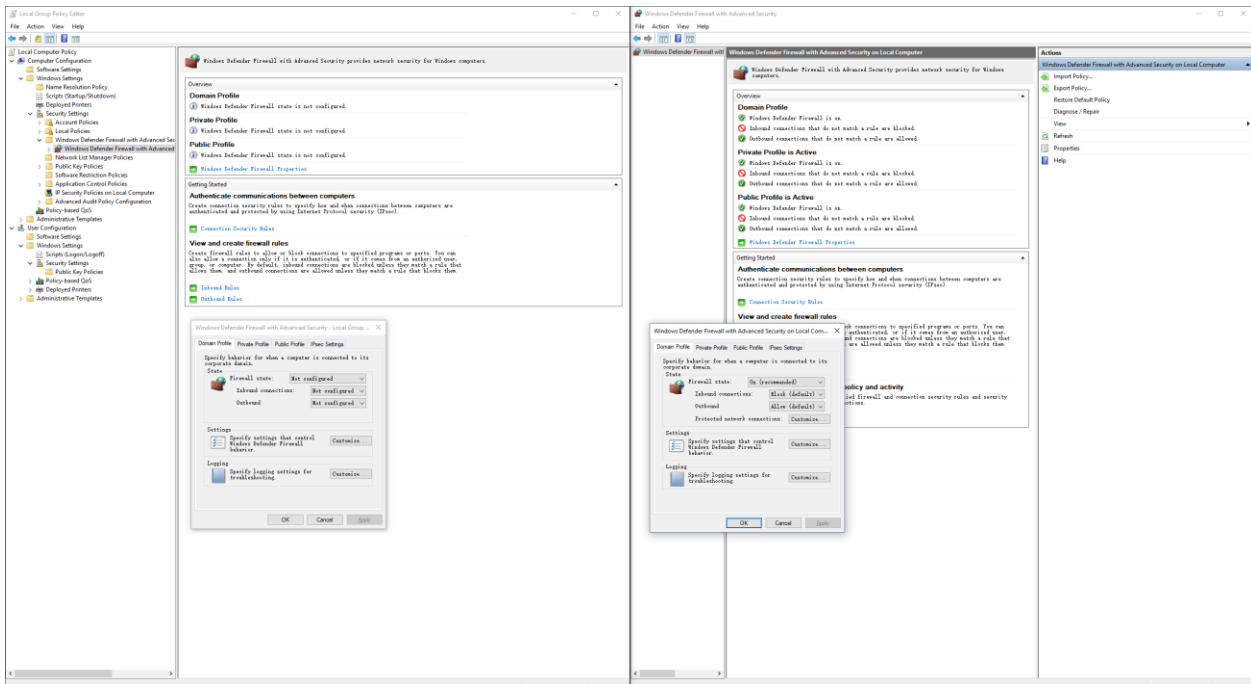


The image shows two screenshots of Windows Firewall configuration. The top screenshot shows the Registry Editor with the path `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy` expanded. The right pane shows a list of firewall rules with columns for Name, Type, and Data. The bottom screenshot shows the Windows Defender Firewall with Advanced Security console. The left pane shows the Firewall Policy tree, and the right pane shows the list of firewall rules. A small dialog box is open over the Firewall Policy tree, showing the 'FirewallPolicy' value.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisableStatefulFTP	REG_DWORD	0x00000000 (0)
DisableStatefulPPTP	REG_DWORD	0x00000000 (0)
IPSecExempt	REG_DWORD	0x00000009 (9)
PolicyVersion	REG_DWORD	0x0000021b (539)

可以看到是一样的。

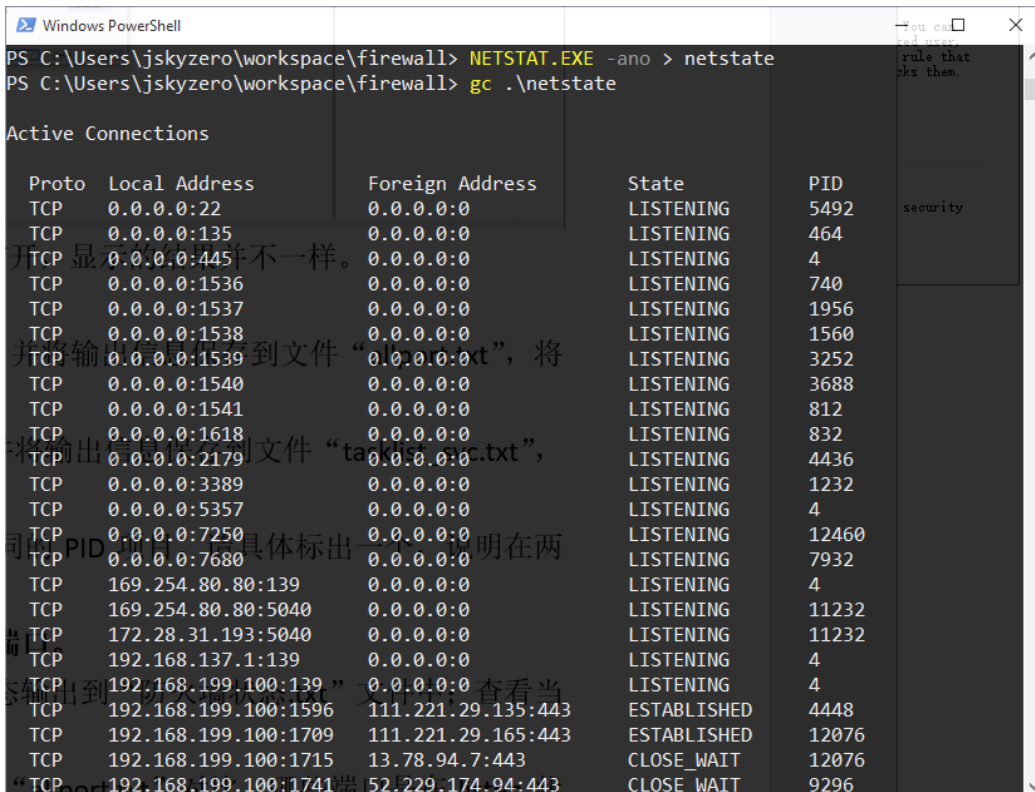
(3) 使用组策略工具（在 cmd 窗口中输入 `gpedit.msc`）查询防火墙配置，并与（1）、（2）作比较。



组策略也可以看到对应的设置，但是似乎是没有以管理员打开，显示的结果并不一样。

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。

Windows PowerShell

Type "TASKLIST /?" for usage.

PS C:\Users\jskyzero\workspace\firewall> tasklist.exe -svc > tasklist

PS C:\Users\jskyzero\workspace\firewall> gc .\tasklist

Image Name	PID	Services
System Idle Process	0	N/A
System	4	N/A
Secure System	56	N/A
smss.exe	424	N/A
csrss.exe	652	N/A
wininit.exe	740	N/A
csrss.exe	748	N/A
services.exe	812	N/A
lsass.exe	832	KeyIso, SamSs, VaultSvc
svchost.exe	956	PlugPlay
svchost.exe	980	BrokerInfrastructure, DcomLaunch, Power, SystemEventsBroker
fontdrvhost.exe	988	N/A
winlogon.exe	580	N/A
svchost.exe	464	RpcEptMapper, RpcSs
fontdrvhost.exe	888	N/A
svchost.exe	1048	LSM
dwm.exe	1152	N/A
svchost.exe	1232	TermService
svchost.exe	1288	lmhosts
svchost.exe	1296	bthserv
svchost.exe	1392	NcbService
svchost.exe	1404	TimeBrokerSvc
svchost.exe	1472	HvHost

(4) 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。

The screenshot shows a Windows PowerShell session with the following commands and outputs:

```
PS C:\Users\jskyzero\workspace\firewall> tasklist.exe -svc | Select-String "Chrome"
```

Process Name	PID	Architecture
chrome.exe	4980	N/A
chrome.exe	3096	N/A
chrome.exe	9408	N/A
chrome.exe	10408	N/A
chrome.exe	4140	N/A
chrome.exe	8432	N/A
chrome.exe	7876	N/A
chrome.exe	10256	N/A
chrome.exe	10532	N/A
chrome.exe	4256	N/A
chrome.exe	7652	N/A
chrome.exe	8068	N/A
chrome.exe	12540	N/A
chrome.exe	4812	N/A

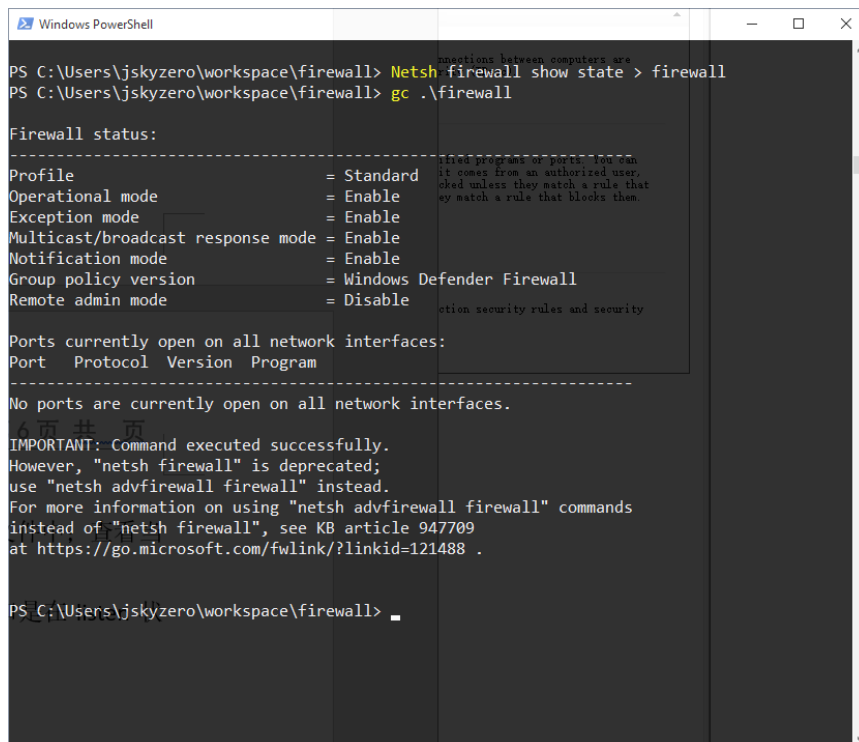
```
PS C:\Users\jskyzero\workspace\firewall> NETSTAT.EXE -ano | Select-String "4980"
```

Protocol	Local Address	Foreign Address	State	PID
TCP	192.168.199.100:2524	64.233.189.188:5228	ESTABLISHED	4980
TCP	192.168.199.100:2532	172.217.24.35:443	ESTABLISHED	4980
TCP	192.168.199.100:2540	216.58.199.110:443	ESTABLISHED	4980
TCP	192.168.199.100:2542	183.240.17.137:80	CLOSE_WAIT	4980
TCP	192.168.199.100:2546	216.58.199.106:443	ESTABLISHED	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	0.0.0.0:5353	*	*	4980
UDP	[::]:5353	*	*	4980

对应关系就是该程序使用了那些端口。

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。



```
Windows PowerShell
PS C:\Users\jskyzero\workspace\firewall> Netsh firewall show state > firewall
PS C:\Users\jskyzero\workspace\firewall> gc .\firewall

Firewall status:
-----
Profile                               = Standard
Operational mode                      = Enable
Exception mode                       = Enable
Multicast/broadcast response mode    = Enable
Notification mode                    = Enable
Group policy version                  = Windows Defender Firewall
Remote admin mode                    = Disable

Ports currently open on all network interfaces:
Port  Protocol  Version  Program
-----
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

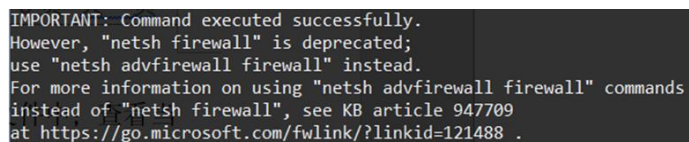
PS C:\Users\jskyzero\workspace\firewall>
```

(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。

如上图所示，防火墙状态中没有打开端口，推测可能存在的问题是应用程序无法在对应端口获得信息。

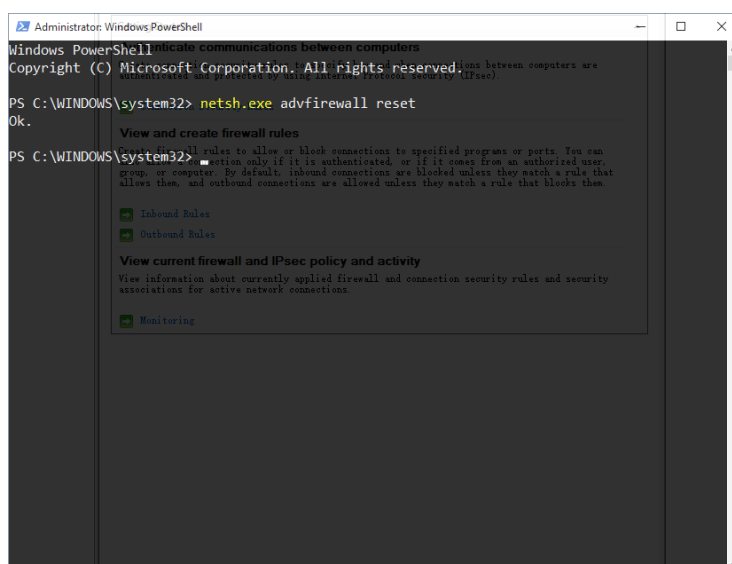
4. 通过防火墙命令 netsh firewall，对防火墙进行管理和配置。

firewall 似乎是很久的指令了，如下图。



```
IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .
```

(1) 恢复默认设置，请说明此操作的必要性；



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\WINDOWS\system32> netsh.exe advfirewall reset
Ok.
View and create firewall rules
PS C:\WINDOWS\system32>
View current firewall and IPsec policy and activity
Monitoring
```

必要性:方便接下来查看配置和不同。

(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；

The screenshot shows the Windows Defender Firewall control panel window. The left sidebar shows the navigation pane with 'Monitoring' selected. The main pane shows the 'Monitoring' tab, indicating that the firewall is on and blocking all inbound connections. A PowerShell window is overlaid on the main pane, showing the command 'netsh.exe firewall set opmode mode = ENABLE exceptions = DISABLE' being executed successfully. The PowerShell window also shows the output of 'netsh advfirewall firewall' commands, which return 'OK'.

(3) 启用防火墙，允许例外；

```
PS C:\WINDOWS\system32> netsh.exe firewall set opmode mode = ENABLE exceptions = enable
IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

Ok.
```

(4) 查询防火墙的参数配置；

Example 1: Enable a program

Old command	New command
netsh firewall add allowedprogram C:\MyApp\MyApp.exe "My Application" ENABLE	netsh advfirewall firewall add rule name="Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes
netsh firewall add allowedprogram program=C:\MyApp\MyApp.exe name="My Application" mode=ENABLE scope=CUSTOM addresses=157.60.0.1,172.16.0.0/16,LocalSubnet profile=Domain	netsh advfirewall firewall add rule name="Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=domain
netsh firewall add allowedprogram program=C:\MyApp\MyApp.exe name="My Application" mode=ENABLE scope=CUSTOM addresses=157.60.0.1,172.16.0.0/16,LocalSubnet profile=ALL	Run the following commands: netsh advfirewall firewall add rule name="Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=domain netsh advfirewall firewall add rule name="Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=private

For more information about how to add firewall rules, run the following command:
netsh advfirewall firewall add rule ?

Example 2: Enable a port

Old command	New command
netsh firewall add portopening TCP 80 "Open Port 80"	netsh advfirewall firewall add rule name="Open Port 80" dir=in action=allow protocol=TCP localport=80

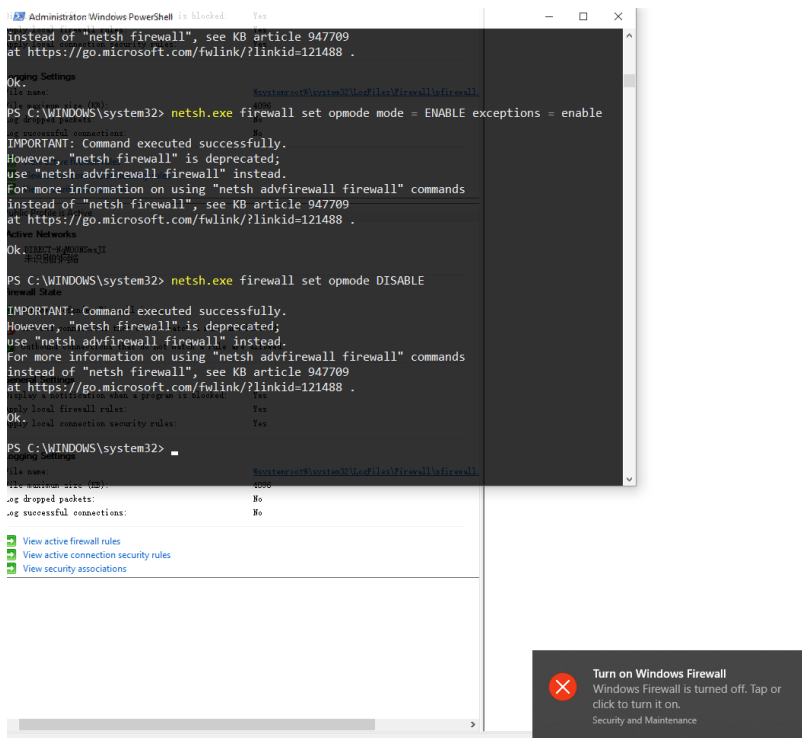
For more information about how to add firewall rules, run the following command:
netsh advfirewall firewall add rule ?

Example 3: Delete enabled programs or ports

Old command	New command
netsh firewall delete allowedprogram C:\MyApp\MyApp.exe	netsh advfirewall firewall delete rule name=rule name program="C:\MyApp\MyApp.exe"
delete portopening protocol=UDP port=500	netsh advfirewall firewall delete rule name=rule name protocol=udp localport=500

For more information about how to delete firewall rules, run the following command:
netsh advfirewall firewall delete rule ?

(5) 关闭防火墙，请说明此操作的必要性。



必要性或许是方便应用透过防火墙，和自己配置防火墙。

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。

图形界面，简单，适合没有基础的用户。

命令行界面，复杂，适合管理员和脚本配置。

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。

第三方的防火墙一般带有更多自动的配置，比如 360 的网络管理。

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。

防火墙可能会直接过滤掉数据包，此时理论上抓包软件是抓不到的。

能顺利透过防火墙的数据包和正常抓包效果应该是一样的。

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。

防火墙分为很多种，比如基本的包过滤防火墙是通过包的信息来过滤，比如包头的 ip 地址端口网络层协议等。而状态检测防火墙通过检查连接状态来过滤，应用代理防火墙通过代理来解决。