

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	2015 级电子政务	学号	15331191	姓名	廖颖泓
完成日期： 2017 年 12 月 13 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 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）。



Windows 10 防火墙

Windows 防火墙是 Windows 操作系统里的其中一个组件，为系统提供一般防火墙的功能。Windows 防火墙内置有安全性记录功能，能把连接的 IP 地址及其他相关数据记录下来。它同时能被设成把截取下来或是允许通过的连接记录下来，因此也可以作为例如追踪电脑曾经浏览过什么网站之类的功能。这个功能默认是关闭的，必须由系统管理员先行激活。

Windows 防火墙最先于 Windows XP SP2 被引入。默认每种连接，例如区域连接、无线网络或 IEEE

1394 也会激活防火墙功能。用户除了能在每种网络连接上直接设置防火墙功能外，更能在组群规则里对防火墙进行更深入更高级的设置。不过 Windows XP 版本的防火墙只能封锁连入连接，而不会封锁连出连接。

Windows Vista 以后版本的 Windows 防火墙在功能上被加强了，使其能更有弹性地集成在操作系统环境中。跟 Windows XP 的防火墙相比，它多出了如下功能：

1. 提供一个叫“Windows 防火墙”的控制台功能，允许对防火墙作更高级的设置，甚至提供远程管理功能。可以在开始->运行输入“wf.msc”以引导这个控制台；

2. IPv6 连接的过滤功能；

3. 连出连接的过滤功能；

4. 高级的数据包过滤功能，允许新增基于来源、目的地 IP 地址或连接端口编号的过滤规则；

5. IPsec 被集成；

6. 界面被增强，允许设立及管理多个防火墙设置。

如今的 Windows 10 防火墙普遍有如下功能：

1. 允许程序或功能通过 Windows 防火墙。用户可以在专用网络和公用网络下，对应用程序是否可以运行进行不同设置；

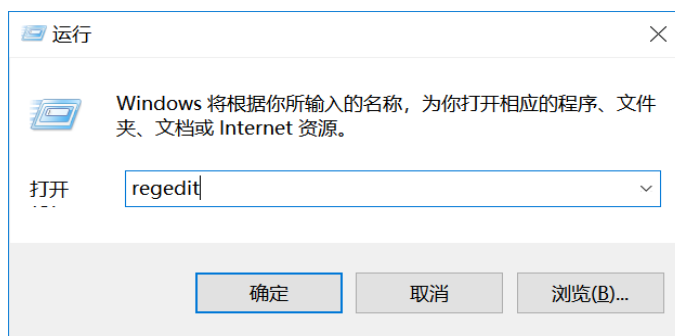
2. 用户可以更改专用和公用网络下的、防火墙开启设置及通知设置；

3. 允许还原默认设置；

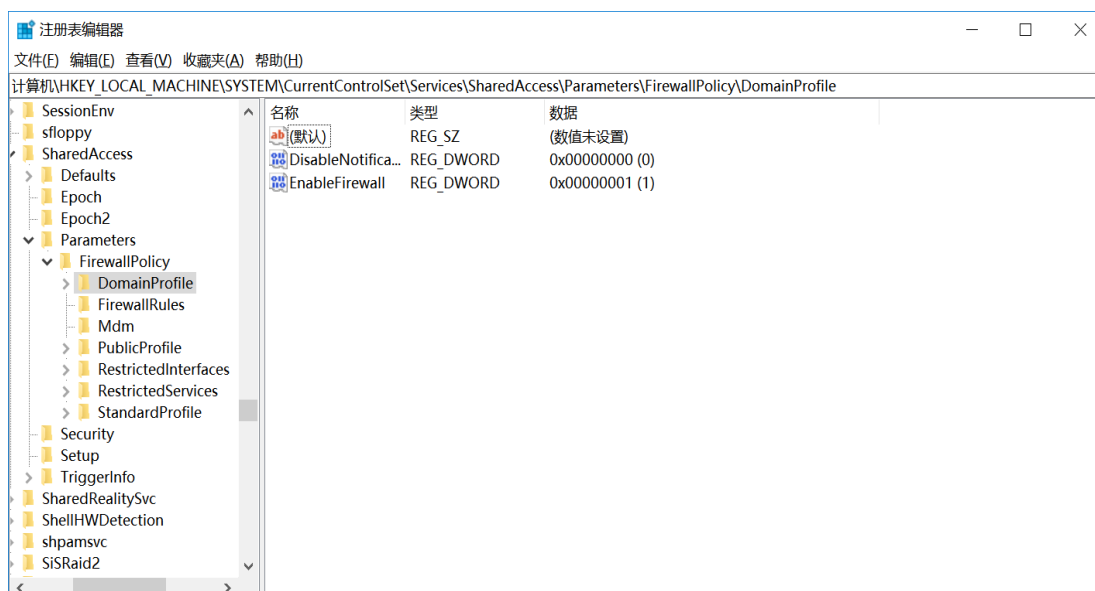
4. 允许用户在高级设置中进行自定义配置；

5. 具备防火墙的一般功能，如保护用户免受非法入侵等。

(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。



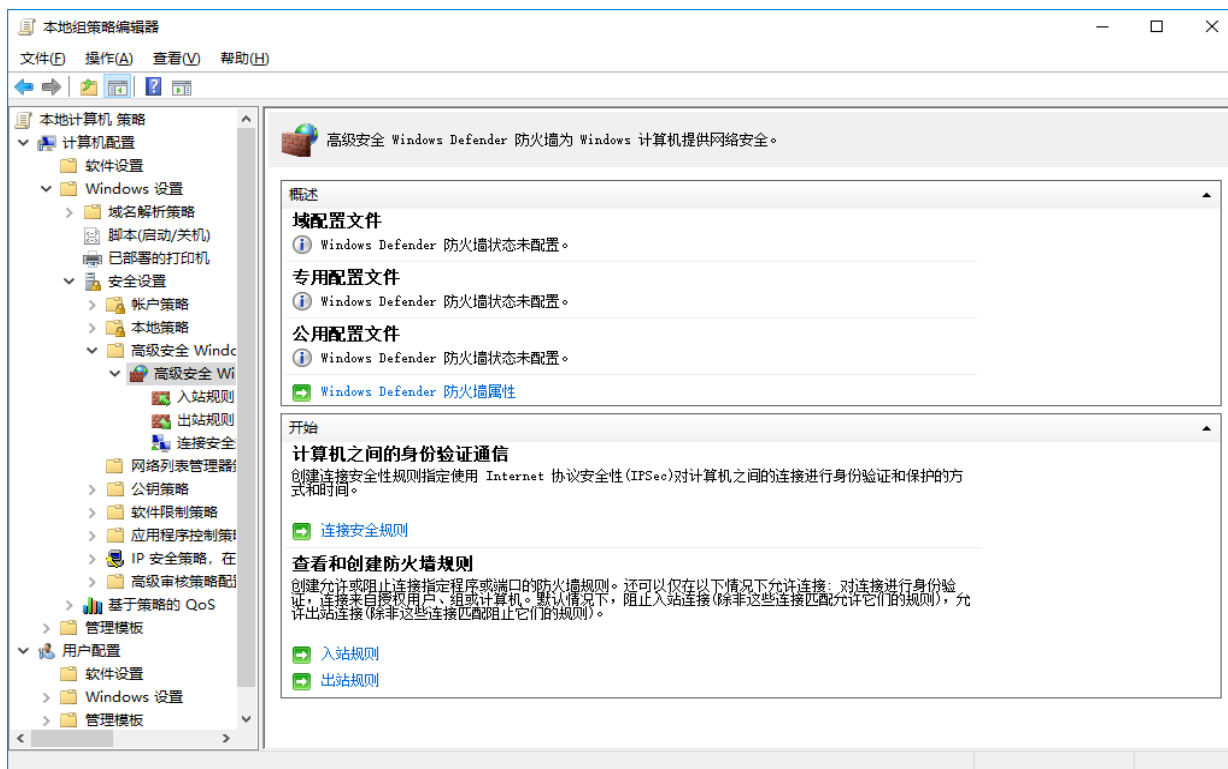
在 cmd 窗口中输入 regedit



注册表中防火墙配置

注册表中防火墙配置的总项位于注册表 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainFile`，与（1）中的结果相比较，注册表中防火墙配置的总项只显示了防火墙是否开启，没有显示在图形界面中包含的例如防火墙具体在何种网络类型中使用、允许哪些程序通过之类的信息。

（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。

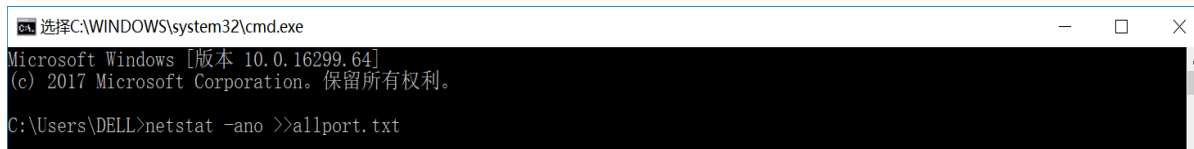


组策略工具查询防火墙配置

组策略工具中的防火墙配置与（1）中的图形界面相比，缺少了通知设置和高级设置，但是仍然可以设置防火墙安全规则，配置防火墙状态；与（2）中的注册表相比，多了防火墙网络分类设置和查看创建防火墙安全规则。

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。



使用 `netstat` 命令（带参数 `-ano`）输出端口信息



allport.txt - 记事本

文件(E) 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	4620	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	588	
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	736	
TCP	0.0.0.0:1537	0.0.0.0:0	LISTENING	1560	
TCP	0.0.0.0:1538	0.0.0.0:0	LISTENING	1576	
TCP	0.0.0.0:1539	0.0.0.0:0	LISTENING	2096	
TCP	0.0.0.0:1540	0.0.0.0:0	LISTENING	3596	
TCP	0.0.0.0:1545	0.0.0.0:0	LISTENING	824	
TCP	0.0.0.0:1546	0.0.0.0:0	LISTENING	808	
TCP	0.0.0.0:1548	0.0.0.0:0	LISTENING	5688	
TCP	0.0.0.0:2382	0.0.0.0:0	LISTENING	4128	
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	4412	
TCP	127.0.0.1:1542	127.0.0.1:5354	ESTABLISHED	4028	
TCP	127.0.0.1:1543	127.0.0.1:5354	ESTABLISHED	4028	
TCP	127.0.0.1:4300	0.0.0.0:0	LISTENING	13660	
TCP	127.0.0.1:4301	0.0.0.0:0	LISTENING	13660	
TCP	127.0.0.1:5354	0.0.0.0:0	LISTENING	3088	
TCP	127.0.0.1:5354	127.0.0.1:1542	ESTABLISHED	3088	
TCP	127.0.0.1:5354	127.0.0.1:1543	ESTABLISHED	3088	
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING	4104	
TCP	127.0.0.1:5939	127.0.0.1:9320	ESTABLISHED	4104	
TCP	127.0.0.1:5939	127.0.0.1:9863	ESTABLISHED	4104	
TCP	127.0.0.1:9190	127.0.0.1:27015	ESTABLISHED	16164	
TCP	127.0.0.1:9320	127.0.0.1:5939	ESTABLISHED	7588	
TCP	127.0.0.1:9325	127.0.0.1:9326	ESTABLISHED	7588	
TCP	127.0.0.1:9326	127.0.0.1:9325	ESTABLISHED	7588	
TCP	127.0.0.1:9863	127.0.0.1:5939	ESTABLISHED	8908	
TCP	127.0.0.1:9990	0.0.0.0:0	LISTENING	3144	
TCP	127.0.0.1:10000	0.0.0.0:0	LISTENING	5944	
TCP	127.0.0.1:27015	0.0.0.0:0	LISTENING	4028	
TCP	127.0.0.1:27015	127.0.0.1:9190	ESTABLISHED	4028	
TCP	127.0.0.1:27018	0.0.0.0:0	LISTENING	11476	
TCP	127.0.0.1:58151	0.0.0.0:0	LISTENING	5964	
TCP	172.18.158.140:139	0.0.0.0:0	LISTENING	4	
TCP	172.18.158.140:9215	111.221.29.98:443	ESTABLISHED	4208	
TCP	172.18.158.140:9862	120.76.248.211:5938	ESTABLISHED	4104	
TCP	172.18.158.140:10176	112.90.84.112:80	ESTABLISHED	13660	
TCP	172.18.158.140:10272	183.232.84.85:80	CLOSE_WAIT	13660	
TCP	172.18.158.140:10789	111.47.223.146:80	ESTABLISHED	13660	
TCP	172.18.158.140:10790	111.221.29.254:443	TIME_WAIT	0	
TCP	172.18.158.140:10791	111.221.29.254:443	TIME_WAIT	0	
TCP	172.18.158.140:10793	111.47.224.153:80	TIME_WAIT	0	
TCP	172.18.158.140:10794	183.232.119.210:80	TIME_WAIT	0	
TCP	172.18.158.140:10795	183.232.175.160:80	ESTABLISHED	13660	
TCP	172.18.158.140:10796	221.179.183.17:80	TIME_WAIT	0	
TCP	[::]:22	[::]:0	LISTENING	4620	
TCP	[::]:80	[::]:0	LISTENING	4	
TCP	[::]:135	[::]:0	LISTENING	588	
TCP	[::]:445	[::]:0	LISTENING	4	
TCP	[::]:1536	[::]:0	LISTENING	736	
TCP	[::]:1537	[::]:0	LISTENING	1560	
TCP	[::]:1538	[::]:0	LISTENING	1576	
TCP	[::]:1540	[::]:0	LISTENING	3596	
TCP	[::]:1545	[::]:0	LISTENING	824	
TCP	[::]:1546	[::]:0	LISTENING	808	
TCP	[::]:1548	[::]:0	LISTENING	5688	
TCP	[::]:2382	[::]:0	LISTENING	4128	
TCP	[::]:3306	[::]:0	LISTENING	4412	
TCP	[::1]:58151	[::]:0	LISTENING	5964	
TCP	[2001:250:3002:4610:942f:bdd0:36af:102e]:9323	[2a00:11c0:31:351::9]:5938	ESTABLISHED	41	
TCP	[2001:250:3002:4610:942f:bdd0:36af:102e]:9902	[2404:6800:4008:c05::bc]:5228	ESTABLISHED		
UDP	0.0.0.0:123	**:		13152	
UDP	0.0.0.0:500	**:		4284	
UDP	0.0.0.0:1434	**:		4128	
UDP	0.0.0.0:4500	**:		4284	
UDP	0.0.0.0:5050	**:		7644	
UDP	0.0.0.0:5353	**:		2996	
UDP	0.0.0.0:5353	**:		8576	
UDP	0.0.0.0:5353	**:		8576	

UDP	0.0.0.0:5353	*:*	8576	
UDP	0.0.0.0:5355	*:*	2996	
UDP	0.0.0.0:20102	*:*	2016	
UDP	0.0.0.0:49664	*:*	3088	
UDP	0.0.0.0:49667	*:*	3048	
UDP	0.0.0.0:49672	*:*	2016	
UDP	0.0.0.0:50574	*:*	13660	
UDP	0.0.0.0:50575	*:*	13660	
UDP	0.0.0.0:53664	*:*	4104	
UDP	0.0.0.0:62395	*:*	4116	
UDP	127.0.0.1:1900	*:*	4276	
UDP	127.0.0.1:49300	*:*	14728	
UDP	127.0.0.1:49666	*:*	4460	
UDP	127.0.0.1:49668	*:*	4028	
UDP	127.0.0.1:49669	*:*	4028	
UDP	127.0.0.1:54249	*:*	4276	
UDP	127.0.0.1:60377	*:*	16164	
UDP	127.0.0.1:60378	*:*	16164	
UDP	172.18.158.140:137	*:*	4	
UDP	172.18.158.140:138	*:*	4	
UDP	172.18.158.140:1900	*:*	4276	
UDP	172.18.158.140:2177	*:*	9780	
UDP	172.18.158.140:5353	*:*	3088	
UDP	172.18.158.140:5353	*:*	4104	
UDP	172.18.158.140:10102	*:*	2016	
UDP	172.18.158.140:54248	*:*	4276	
UDP	:::123	*:*	13152	
UDP	:::500	*:*	4284	
UDP	:::1434	*:*	4128	
UDP	127.0.0.1:60378	*:*	16164	
UDP	172.18.158.140:137	*:*	4	
UDP	172.18.158.140:138	*:*	4	
UDP	172.18.158.140:1900	*:*	4276	
UDP	172.18.158.140:2177	*:*	9780	
UDP	172.18.158.140:5353	*:*	3088	
UDP	172.18.158.140:5353	*:*	4104	
UDP	172.18.158.140:10102	*:*	2016	
UDP	172.18.158.140:54248	*:*	4276	
UDP	:::123	*:*	13152	
UDP	:::500	*:*	4284	
UDP	:::1434	*:*	4128	
UDP	:::4500	*:*	4284	
UDP	:::5353	*:*	8576	
UDP	:::5353	*:*	8576	
UDP	:::5353	*:*	2996	
UDP	:::5355	*:*	2996	
UDP	:::49665	*:*	3088	
UDP	:::53665	*:*	4104	
UDP	:::1]:1900	*:*	4276	
UDP	:::1]:5353	*:*	4104	
UDP	:::1]:5353	*:*	3088	
UDP	:::1]:54247	*:*	4276	
UDP	[2001:250:3002:4610:942f:bdd0:36af:102e]:2177	*:*		9780
UDP	[2001:250:3002:4610:e0d4:3365:3ae8:b91f]:2177	*:*		9780
UDP	[fe80::e0d4:3365:3ae8:b91f%2]:1900	*:*	4276	
UDP	[fe80::e0d4:3365:3ae8:b91f%2]:2177	*:*	9780	
UDP	[fe80::e0d4:3365:3ae8:b91f%2]:54246	*:*	4276	

文件“allport.txt”中的端口信息

(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。

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.16299.64]
(c) 2017 Microsoft Corporation. 保留所有权利。
C:\Users\DELL>tasklist -svc >>tasklist_svc.txt
  
```

使用 tasklist 命令（带参数 svc）获得进程信息

tasklist_svc.txt - 记事本			—	□	×
文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)					
映像名称	PID	服务			
System Idle Process	0	暂缺			
System	4	暂缺			
smss.exe	416	暂缺			
csrss.exe	628	暂缺			
wininit.exe	736	暂缺			
services.exe	808	暂缺			
lsass.exe	824	KeyIso, SamSs, VaultSvc			
svchost.exe	936	PlugPlay			
svchost.exe	960	BrokerInfrastructure, DcomLaunch, Power, SystemEventsBroker			
fontdrvhost.exe	984	暂缺			
svchost.exe	588	RpcEptMapper, RpcSs			
svchost.exe	1028	LSM			
svchost.exe	1188	TermService			
svchost.exe	1280	NcbService			
svchost.exe	1348	hidserv			
svchost.exe	1380	TimeBrokerSvc			
svchost.exe	1496	ProfSvc			
svchost.exe	1560	EventLog			
svchost.exe	1576	Schedule			
svchost.exe	1696	UserManager			
svchost.exe	1772	nsi			
svchost.exe	1828	Dhcp			
svchost.exe	1896	lfsvc			
svchost.exe	1904	CertPropSvc			
svchost.exe	1948	BFE, CoreMessagingRegistrar, MpsSvc			
svchost.exe	804	NlaSvc			
svchost.exe	1260	LanmanWorkstation			
svchost.exe	2096	SessionEnv			
svchost.exe	2196	netprofm			
nvsvc.exe	2384	nvsvc			
svchost.exe	2408	Themes			
svchost.exe	2412	SysMain			
svchost.exe	2424	EventSystem			
svchost.exe	2504	SENS			
Memory Compression	2528	暂缺			
igfxCUIService.exe	2564	igfxCUIService2.0.0.0			
svchost.exe	2608	AudioEndpointBuilder			
svchost.exe	2616	FontCache			
svchost.exe	2708	Winmgmt			
svchost.exe	2776	Audiosrv			
svchost.exe	2836	StateRepository			
RtkAudioService64.exe	2888	RtkAudioService			
WavesSysSvc64.exe	2908	WavesSysSvc			
svchost.exe	2996	Dnscache			
svchost.exe	3004	Wcmsvc			
svchost.exe	3012	DusmSvc			
svchost.exe	3152	Eaphost			
svchost.exe	3260	WinHttpAutoProxySvc			
svchost.exe	3400	dot3svc			
svchost.exe	3408	WlanSvc			
svchost.exe	3512	ShellHWDetection			
spoolsv.exe	3596	Spooler			
wlanext.exe	3684	暂缺			
conhost.exe	3708	暂缺			
AppleMobileDeviceService.	4028	Apple Mobile Device Service			
EvtEng.exe	4040	EvtEng			
mDNSResponder.exe	3088	Bonjour Service			
armsvc.exe	3104	AdobeARMSvc			
AuthenMngService.exe	2016	INODE_SVR_MNG_SERVICE			
RegSrv.exe	2008	RegSrv			
NvNetworkService.exe	3144	NvNetworkService			
QQMicroGameBoxService.exe	3048	QQMicroGameBoxService			
svchost.exe	3548	DeviceAssociationService			
svchost.exe	4108	CryptSvc			
QQProtect.exe	4116	QPCore			
sqlbrowser.exe	4128	SQLBrowser			
RaRegistry.exe	4152	RalinkRegistryWriter			
sqlwriter.exe	4160	SQLWriter			
ibtsiva.exe	4168	ibtsiva			
SynTPEnhService.exe	4200	SynTPEnhService			
svchost.exe	4208	WpnService			
svchost.exe	4216	DiagTrack			

ZeroConfigService.exe	4228	ZeroConfigService
RaAutoInstSrv.exe	4240	RaAutoInstSrv_RT73
svchost.exe	4248	SstpSvc
svchost.exe	4256	TrkWks
svchost.exe	4268	SharedAccess
svchost.exe	4276	SSDPSRV
svchost.exe	4284	IKEEXT
SecurityHealthService.exe	4356	SecurityHealthService
mysqld.exe	4412	MySQL57
svchost.exe	4444	DPS
svchost.exe	4460	iphlpvc
svchost.exe	4752	LanmanServer
svchost.exe	4892	SshBroker
dasHost.exe	4932	暂缺
svchost.exe	4948	WdiServiceHost
svchost.exe	4620	SshProxy
svchost.exe	5232	RasMan
unsecapp.exe	5472	暂缺
WmiPrvSE.exe	5740	暂缺
sqlceip.exe	5948	SSASTELEMTRY\$MYSQLSERVER
sqlceip.exe	5956	SQLTELEMTRY\$MYSQLSERVER
sqlservr.exe	5964	MSSQL\$MYSQLSERVER
sqlceip.exe	5972	SQLTELEMTRY\$MYDATABASE
ReportingServicesService.	6060	ReportServer\$MYSQLSERVER
msmdsrv.exe	5688	MSOLAP\$MYSQLSERVER
iNodeMon.exe	6964	暂缺
svchost.exe	7312	Appinfo
PresentationFontCache.exe	7544	FontCache3.0.0.0
svchost.exe	7736	TokenBroker
svchost.exe	8120	TabletInputService
svchost.exe	8256	PcaSvc
Microsoft.ReportingServic	8684	暂缺
conhost.exe	8736	暂缺
svchost.exe	7644	CDPSvc
svchost.exe	9380	NgcCtnrSvc
svchost.exe	9404	PolicyAgent
svchost.exe	10944	LicenseManager
iPodService.exe	12336	iPod Service
fdlauncher.exe	13280	MSSQLFDLauncher\$MYDATABASE
fdlauncher.exe	10820	MSSQLFDLauncher\$MYSQLSERVER
fdhost.exe	776	暂缺
conhost.exe	848	暂缺
GoogleCrashHandler.exe	4568	暂缺
GoogleCrashHandler64.exe	5824	暂缺
GoogleIMEJaCacheService.e	4724	GoogleIMEJaCacheService
IAStorDataMgrSvc.exe	13160	IAStorDataMgrSvc
svchost.exe	1632	wscsv
svchost.exe	13152	W32Time
svchost.exe	14328	RmSvc
svchost.exe	5496	StorSvc
svchost.exe	1980	upnphost
svchost.exe	2104	DoSvc
svchost.exe	9780	QWAVE
SearchIndexer.exe	14024	WSearch
svchost.exe	3388	seclogon
TeamViewer_Service.exe	4104	TeamViewer
CAJSHost.exe	11476	CAJ Service Host
audiogd.exe	11864	暂缺

文件“tasklist_svc.txt”中的进程信息

(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	[::]:1540	[::]:0	LISTENING	3596	
TCP	[::]:1545	[::]:0	LISTENING	824	
TCP	[::]:1546	[::]:0	LISTENING	808	
TCP	[::]:1548	[::]:0	LISTENING	5688	
TCP	[::]:2382	[::]:0	LISTENING	4128	
TCP	[::]:3306	[::]:0	LISTENING	4412	
TCP	[::1]:58151	[::]:0	LISTENING	5964	
TCP	[2001:250:3002:4610:942f:bdd0:36af:102e]:9323	[2a00:11c0:31:351::9]:5938	ESTABLISHED	41	
TCP	[2001:250:3002:4610:942f:bdd0:36af:102e]:9902	[2404:6800:4008:c05::bc]:5228	ESTABLISHED		
UDP	0.0.0.0:123	*:*		13152	
UDP	0.0.0.0:500	*:*		4284	
UDP	0.0.0.0:1434	*:*		4128	
UDP	0.0.0.0:4500	*:*		4284	
UDP	0.0.0.0:5050	*:*		7644	
UDP	0.0.0.0:5353	*:*		2996	
UDP	0.0.0.0:5353	*:*		8576	
UDP	0.0.0.0:5353	*:*		8576	

文件“allport.txt”中 PID 为 4128 的项目

```
AppleMobileDeviceService. 4028 Apple Mobile Device Service
EvtEng.exe 4040 EvtEng
mDNSResponder.exe 3088 Bonjour Service
armsvc.exe 3104 AdobeARMSvc
AuthenMngService.exe 2016 INODE_SVR_MNG_SERVICE
RegSvc.exe 2008 RegSvc
NvNetworkService.exe 3144 NvNetworkService
QQMicroGameBoxService.exe 3048 QQMicroGameBoxService
svchost.exe 3548 DeviceAssociationService
svchost.exe 4108 CryptSvc
SQLProtect.exe 4116 QPCore
sqlbrowser.exe 4128 SQLBrowser
RaRegistry.exe 4152 RalinkRegistryWriter
sqlwriter.exe 4160 SQLWriter
ibtsiva.exe 4168 ibtsiva
SynTPEnhService.exe 4200 SynTPEnhService
svchost.exe 4208 WpnService
svchost.exe 4216 DiagTrack
```

文件“tasklist_svc.txt”中 PID 为 4128 的项目

PID 为 4128 的进程是 SQL 浏览器，分别使用了 TCP 端口 2382 和 UDP 端口 1434。

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。

```
选择C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.16299.64]
(c) 2017 Microsoft Corporation. 保留所有权利。
C:\Users\DELL>netsh firewall show state >>防火墙状态.txt
```

执行命令 Netsh firewall show state

```
防火墙状态.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

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 Defender 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。
但是, "netsh firewall" 已弃用;
请改用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息, 请参阅
https://go.microsoft.com/fwlink/?linkid=121488 上的 KB 文章 947709。
```

防火墙的状态及端口信息

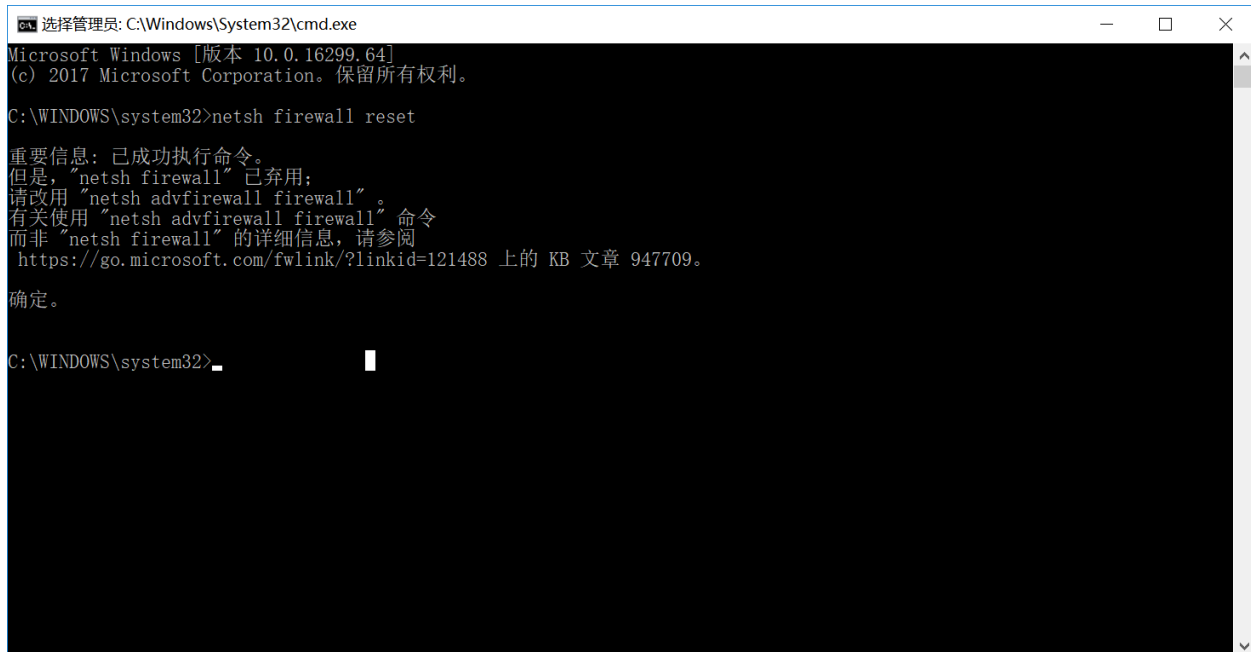
(2) 将“防火墙状态.txt”文件中端口与 2 (1) 的文件“allport.txt”对比，哪些端口是在 listen 状态、但防火墙并没有打开该端口，讨论这样可以发现应用程序存在那些问题。

2 (1) 的文件“allport.txt”中端口 4620、5、88 等端口在 listen 状态，可是防火墙并没有打开这些端口，只打开了 3306 端口。没有打开端口，说明端口被阻塞或被过滤了，该应用程序可能会被利用或涉及到重要信息，为防止泄露而不打开端口

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；

恢复默认设置命令：netsh firewall reset



```
选择管理员: C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.16299.64]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\WINDOWS\system32>netsh firewall reset

重要信息: 已成功执行命令。
但是, "netsh firewall" 已弃用;
请改用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息, 请参阅
https://go.microsoft.com/fwlink/?linkid=121488 上的 KB 文章 947709。

确定。

C:\WINDOWS\system32>_
```

使用命令恢复默认设置

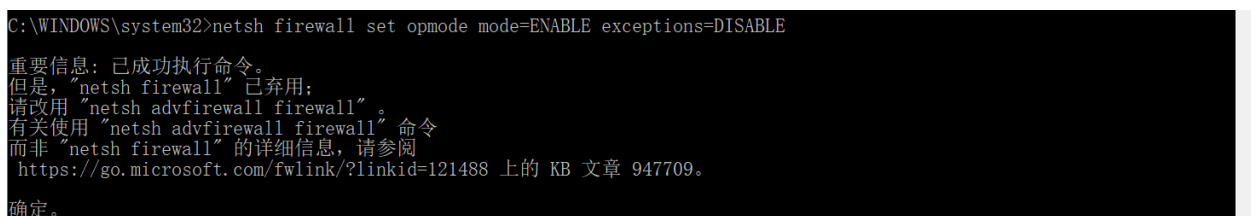
此操作的必要性：当用户配置防火墙不当，发生不可知错误，影响系统运行时，可以通过恢复默认设置来撤销操作。

(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；

启用防火墙并且不允许例外命令：netsh firewall set opmode mode=ENABLE exceptions=DISABLE



启用防火墙前防火墙图形界面



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

重要信息: 已成功执行命令。
但是, "netsh firewall" 已弃用;
请改用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息, 请参阅
https://go.microsoft.com/fwlink/?linkid=121488 上的 KB 文章 947709。

确定。
```

执行命令：netsh firewall set opmode mode=ENABLE exceptions=DISABLE



启用防火墙后防火墙图形界面, 其中来宾或共有网络所有连接被阻止

(3) 启用防火墙, 允许例外;

启用防火墙允许例外命令: `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。
但是, "netsh firewall" 已弃用;
请改用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息, 请参阅
<https://go.microsoft.com/fwlink/?linkid=121488> 上的 KB 文章 947709。
确定。

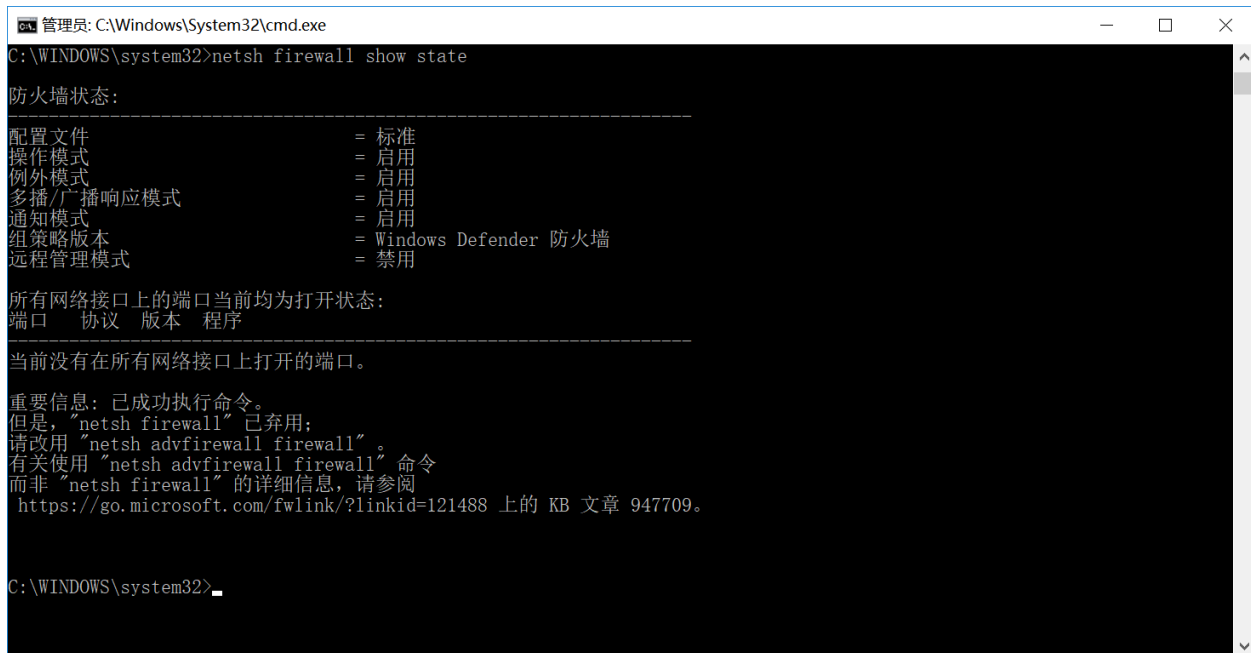
执行命令: `netsh firewall set opmode mode=ENABLE exceptions=ENABLE`



启用防火墙后防火墙图形界面, 其中来宾或共有网络所有连接被阻止取消

(4) 查询防火墙的参数配置;

查询防火墙的参数配置命令: `netsh firewall show state`



```
管理员: C:\Windows\System32\cmd.exe
C:\WINDOWS\system32>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 Defender 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
-----
当前没有在所有网络接口上打开的端口。

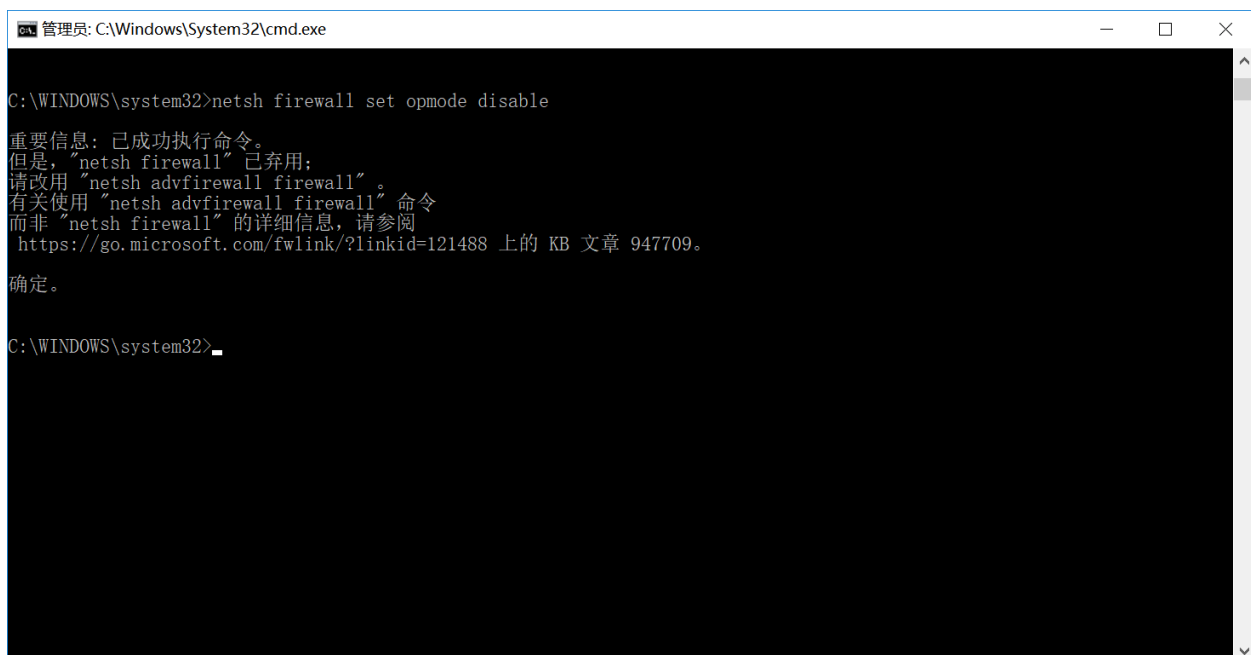
重要信息: 已成功执行命令。
但是, "netsh firewall" 已弃用;
请改用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息, 请参阅
https://go.microsoft.com/fwlink/?linkid=121488 上的 KB 文章 947709。

C:\WINDOWS\system32>
```

执行命令: netsh firewall show state

(5) 关闭防火墙, 请说明此操作的必要性。

关闭防火墙命令: netsh firewall set opmode disable



```
管理员: C:\Windows\System32\cmd.exe
C:\WINDOWS\system32>netsh firewall set opmode disable

重要信息: 已成功执行命令。
但是, "netsh firewall" 已弃用;
请改用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息, 请参阅
https://go.microsoft.com/fwlink/?linkid=121488 上的 KB 文章 947709。

确定。

C:\WINDOWS\system32>
```

执行命令: netsh firewall set opmode disable

此操作的必要性: 当一些必须执行的程序与防火墙产生冲突时, 就需要关闭防火墙, 防止正常的数据包被过滤。

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。

(1) 图形管理方式

优点: 可以提供较多的管理功能、直观方便;

缺点: 需要专门编写图形界面软件, 在远程和集中管理方面不够灵活;

适用场合: 普通用户。

(2) 命令行管理方式

优点：响应快、效率高、专业、易排查故障；

缺点：不直观、使用需要熟悉相关命令；

适用场合：IT 专业人员

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。

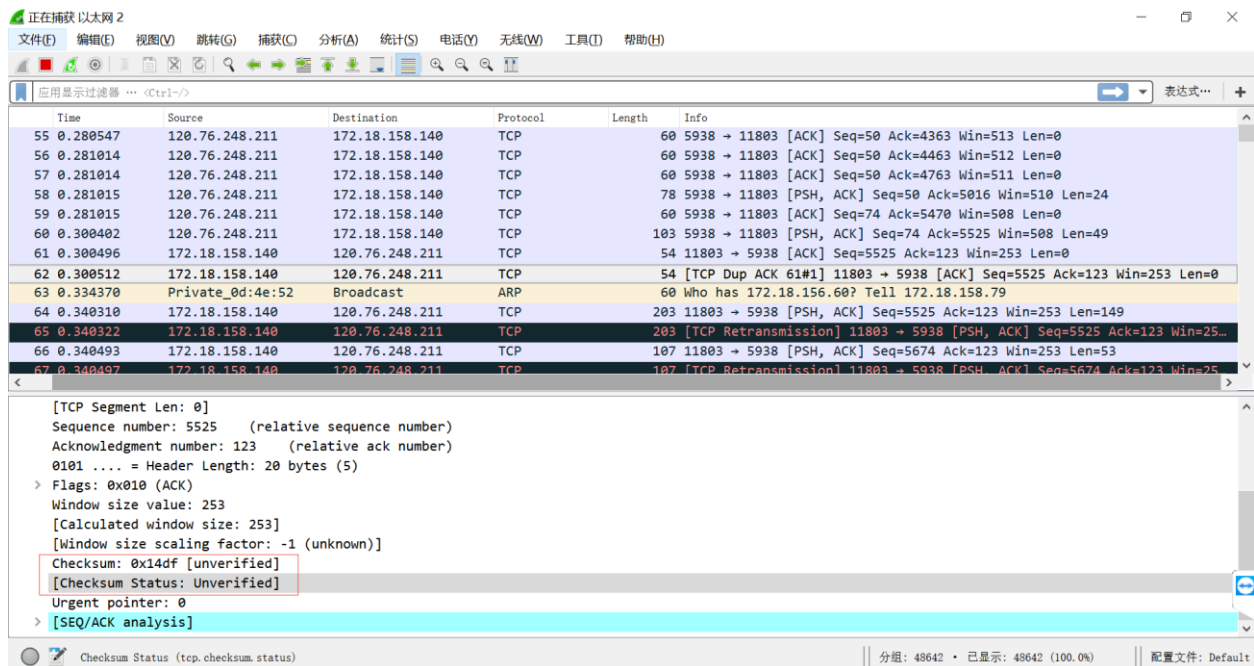
第三方防火墙：火绒防火墙；

相同点：允许用户自定义防火墙规则，允许特殊程序运行；

不同点：火绒防火墙自带网络监控、网络安全、流量统计、网速测试等功能。

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。

当防火墙遇到来源不明的、不可信的数据包时，如校验和未知时，会将数据包丢弃。



Wireshark 捕获到校验和不能确认的包

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。

网络防火墙基于数据包的拦截技术。在Windows下，数据包的拦截方式有很多种，用户级下的数据包拦截方式有：Winsock Layered Service Provider(LSP)；Win2K包过滤接口(Win2KPacketFilteringInterface)；替换Winsock动态链接库(Winsock Replacement DLL)。内核级下的数据包拦截方式有：TDI过滤驱动程序(TDI-Filter Driver)；NDIS中间层驱动程序(NDIS Intermediate Driver)；Win2KFilter-HookDriver。

包过滤防火墙是通过查看数据包的包头来决定丢弃还是接收。数据包过滤由用于内部主机与外部主机之间的过滤系统执行，通常是一台路由器或一台主机。过滤系统的过滤规则基于以下信息：源IP地址、目标IP地址、协议(TCP/UDP/ICMP等)、源端口、目标端口、ICMP消息类型、TCP包头中的ACK位等。包过滤设备端口需存储包过滤规则，应用于包的规则顺序与规则的存储顺序需相同。通过屏蔽特定端口，包过滤系统可以禁止特定服务，阻塞内部主机和外部主机或另一个网络之间的连接。

当包到达端口时，网络防火墙对包头进行语法分析，若一条规则阻止包传输或接收，则包不被允许；若一条规则允许包传输或接收，则包可以继续被处理；若包不满足任一条规则，则被阻塞。