

针对“永恒之蓝”攻击紧急处置手册 (WannaCry 蠕虫)



360安全监测与响应中心

2017 年 05 月 12 日

目录

1 应急处置推荐操作	2
2 隔离网主机应急处置指南	2
2.1 命令行检查端口开放情况	2
2.2 针对 Windows XP 的处置方式	3
2.2.1 方式一：启用蠕虫快速免疫工具	3
2.2.2 方式二：针对主机进行补丁升级	4
2.2.3 方式三：关闭 445 端口相关服务	4
2.2.4 方式四：配置主机级 ACL 策略封堵 445 端口	6
2.3 针对 WIN7 手工处置方式	14
2.3.1 方式一：命令行停止服务	14
2.3.2 方式二：修改注册表	16
2.3.3 方式三：启用 windows 防火墙	21
3 核心网络设备应急处置操作指南	27
3.1 Juniper 设备的建议配置（示例）	27
3.2 华三(H3C)设备的建议配置（示例）	28
3.3 华为设备的建议配置（示例）	30
3.4 Cisco 设备的建议配置（示例）	31
3.5 锐捷设备的建议配置（示例）	31
4 互联网主机应急处置操作指南	32

1 应急处置推荐操作

终端常见处置方式一览表：

Windows XP 处理方式	主机类型	处理措施	效果	效率
<div style="text-align: center;">  </div>	已感染	主机隔离	无法恢复数据	低
	未感染	免疫工具	抑制不被感染	高
	未感染	补丁升级	根除感染可能	低
	未感染	关闭服务	抑制不被感染	低
	未感染	配置 ACL 策略	抑制传播	低

特别提醒，四种处置方式均应确保在未感染主机不联网的情况下操作。

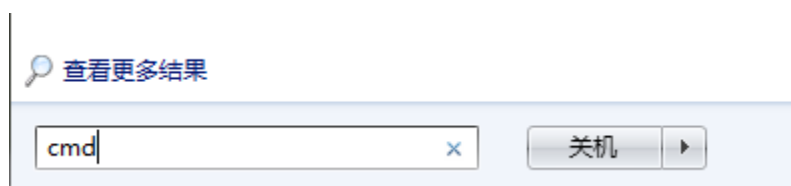
从响应效率和质量上，360 建议首先采用方式一进行抑制，再采用方式二进行根除。

关于如何排查是否已经被感染请参考《“WannaCry”勒索病毒感染特征检查手册》。

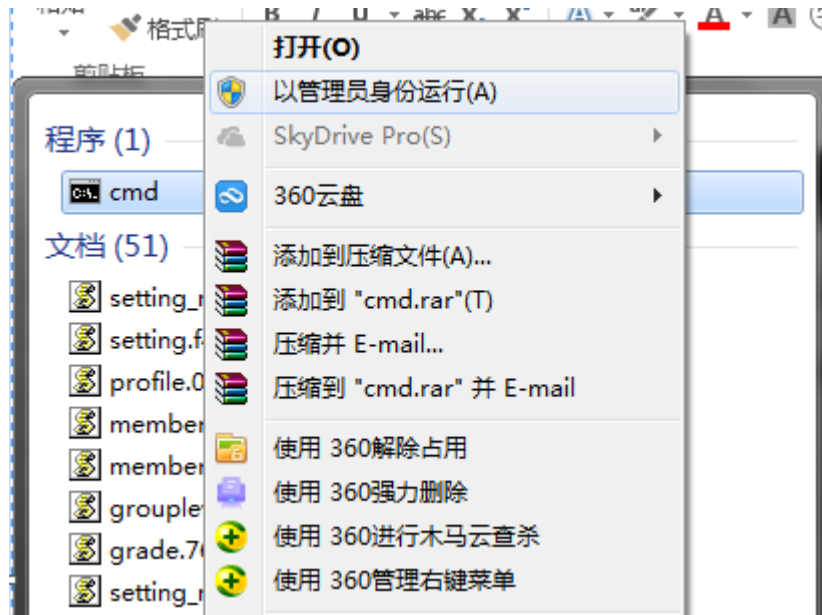
2 隔离网主机应急处置指南

2.1 命令行检查端口开放情况

点击 windows 图标，在搜索框中输入 “cmd”



在搜索结果中的“cmd”上点击右键单击“以管理员身份运行”按钮



在命令行中输入“netstat -an|more”



2.2 针对 Windows XP 的处置方式

2.2.1 方式一：启用蠕虫快速免疫工具

免疫工具的下载地址 <http://dl.b.360.cn/tools/OnionWormImmune.exe>

请双击运行 OnionWormImmune.exe 工具，并检查任务管理器中的状态。



2.2.2 方式二：针对主机进行补丁升级

请参考紧急处置工具包相关目录并安装 MS17-010 补丁，微软已经发布 winxp_sp3 至 win10、win2003 至 win2016 的全系列补丁。

微软官方下载地址（采用已经免疫的电脑下载补丁）：

<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

快速下载地址：

<https://yunpan.cn/cXLwmvHrMF3WI> 访问密码 614d

2.2.3 方式三：关闭 445 端口相关服务

点击开始菜单，运行，cmd，确认。

输入命令 netstat -an 查看端口状态

```

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\admin>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
TCP    127.0.0.1:1029           0.0.0.0:0               LISTENING
TCP    192.168.232.137:139      0.0.0.0:0               LISTENING
UDP    0.0.0.0:445              *:*:
UDP    0.0.0.0:500              *:*:
UDP    0.0.0.0:1025             *:*:
UDP    0.0.0.0:4500             *:*:
UDP    127.0.0.1:123            *:*:
UDP    127.0.0.1:1900           *:*:
UDP    192.168.232.137:123      *:*:
UDP    192.168.232.137:137      *:*:
UDP    192.168.232.137:138      *:*:
UDP    192.168.232.137:1900     *:*:

C:\Documents and Settings\admin>net stop rdr
Workstation 服务正在停止.
  
```

输入 net stop rdr 回车

net stop srv 回车

net stop netbt 回车

```

C:\WINDOWS\system32\cmd.exe
UDP    192.168.232.137:1900     *:*:

C:\Documents and Settings\admin>net stop rdr
Workstation 服务正在停止.
Workstation 服务已成功停止.

C:\Documents and Settings\admin>net stop srv
Server 服务正在停止.
Server 服务已成功停止.

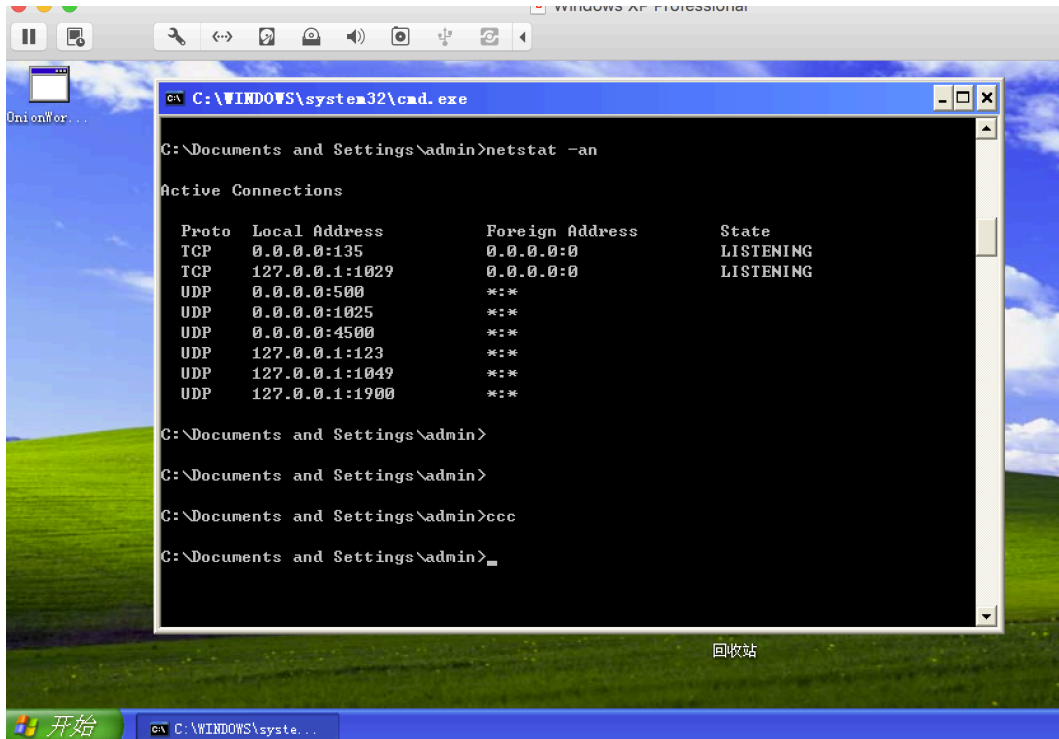
C:\Documents and Settings\admin>net stop netbt
下面的服务依赖于 NetBios over Tcpip 服务:
停止 NetBios over Tcpip 服务也会停止这些服务。

    TCP/IP NetBIOS Helper
    DHCP Client

是否继续此操作? (Y/N) [N]: y
TCP/IP NetBIOS Helper 服务已成功停止.

DHCP Client 服务正在停止.
DHCP Client 服务已成功停止.
  
```

再次输入 netstat -an，成功关闭 445 端口。

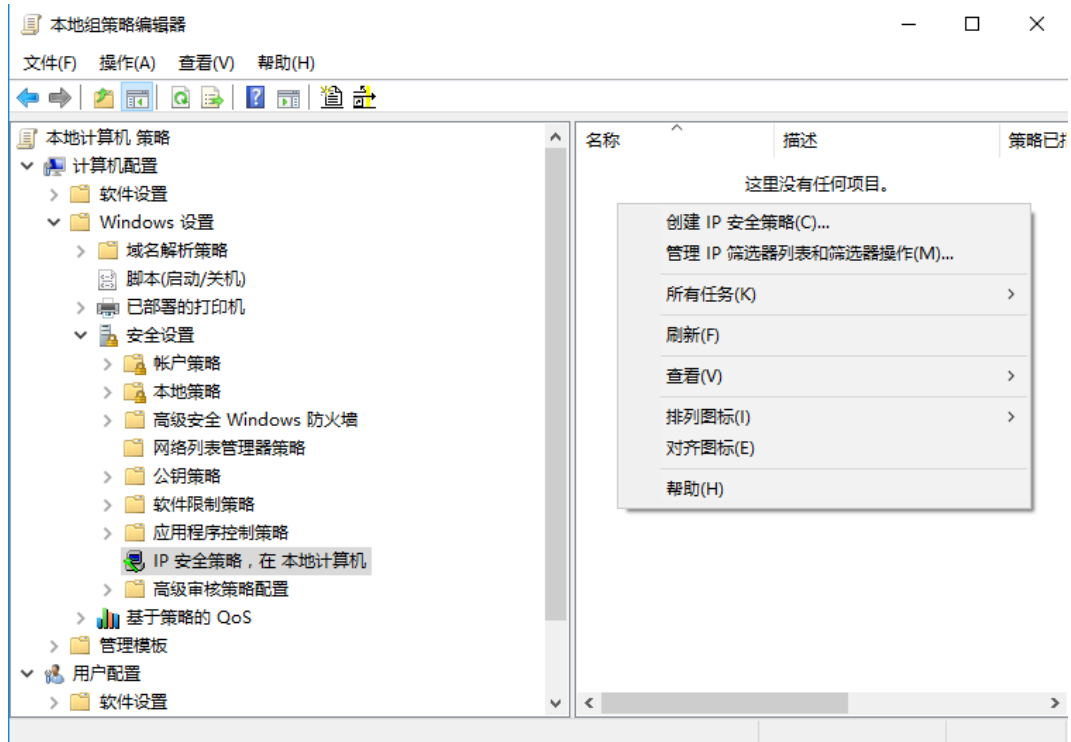


2.2.4 方式四：配置主机级 ACL 策略封堵 445 端口

通过组策略 IP 安全策略限制 Windows 网络共享协议相关端口

开始菜单->运行，输入 gpedit.msc 回车。打开组策略编辑器

在组策略编辑器中，计算机配置->windows 设置->安全设置->ip 安全策略 下，在编辑器右边空白处鼠标右键单击，选择“创建 IP 安全策略”



下一步->名称填写“封端口”，下一步->下一步->勾选编辑属性，并点完成



去掉“使用添加向导”的勾选后，点击“添加”



在新弹出的窗口，选择“IP 筛选列表”选项卡，点击“添加”



在新弹出的窗口中填写名称，去掉“使用添加向导”前面的勾，单击“添加”

IP 筛选器列表

IP 筛选器列表由多个筛选器组成。这样，多个子网、IP 地址和协议可被整合到一个 IP 筛选器中。

名称(N): 端口过滤

描述(D):

添加(A)...

编辑(E)...

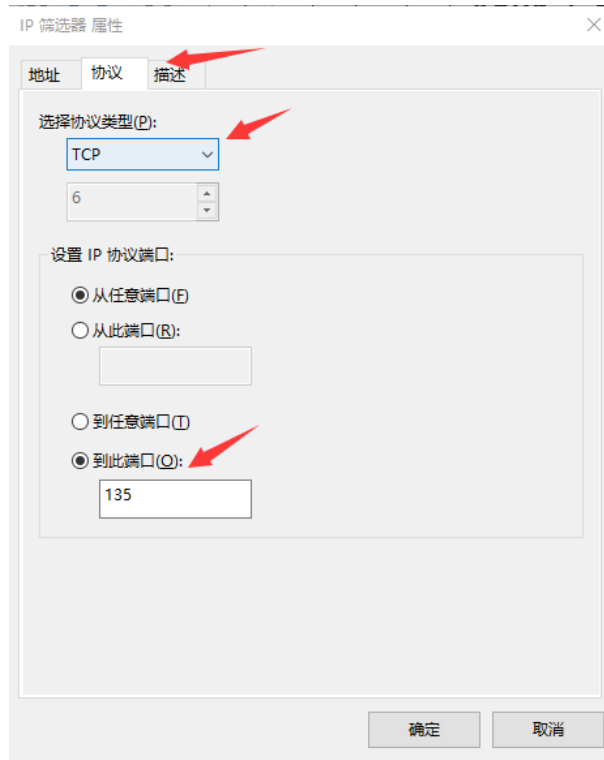
删除(R)

IP 筛选器(S): ☐ 使用“添加向导”(W)

镜像	描述	源 DNS 名称	源地址	目标 DNS 名称
----	----	----------	-----	-----------

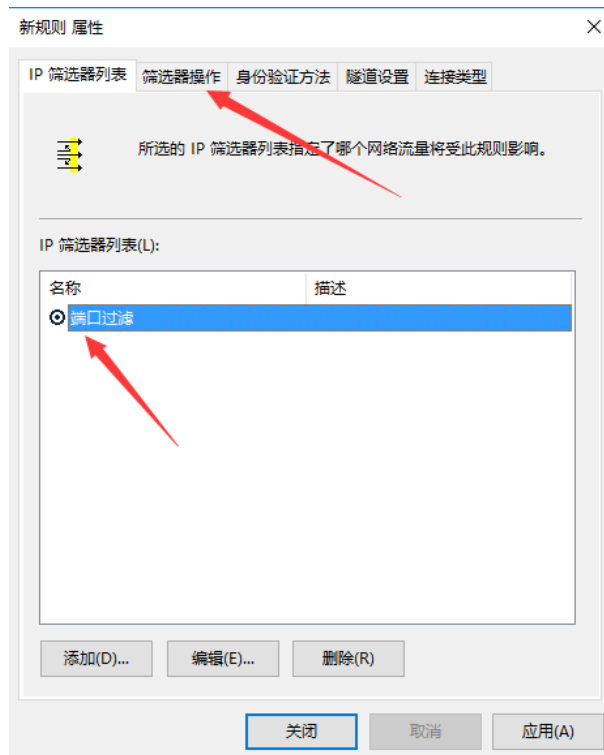
确定 取消

在新弹出的窗口中，“协议”选项卡下，选择协议和设置到达端口信息，并点确定。



重复第 7 个步骤，添加 TCP 端口 135、139、445。添加 UDP 端口 137、138。添加全部完成后，确定。

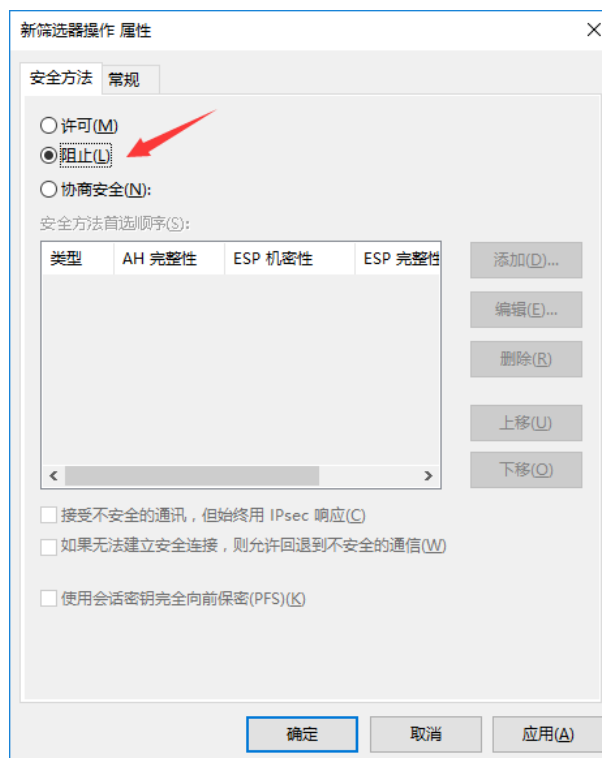
选中刚添加完成的“端口过滤”规则，然后选择“筛选器操作”选项卡。



去掉“使用添加向导”勾选，单击“添加”按钮



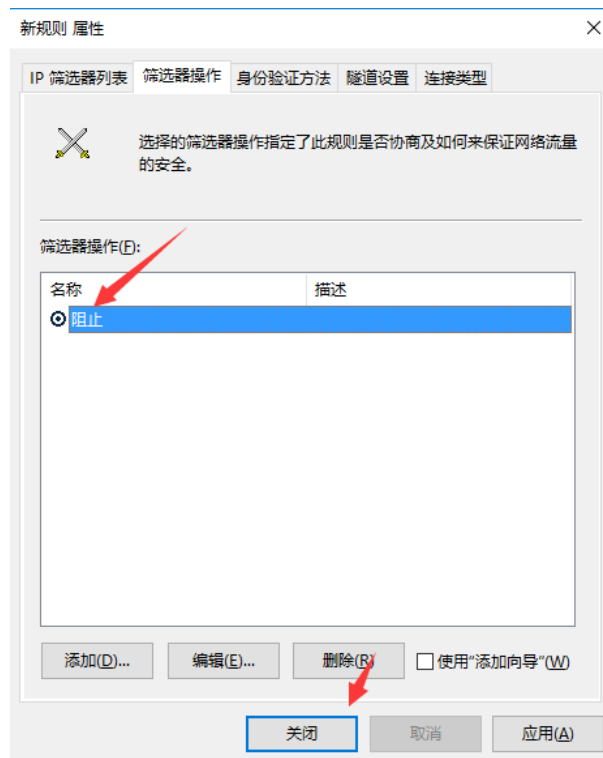
1. 选择“阻止”



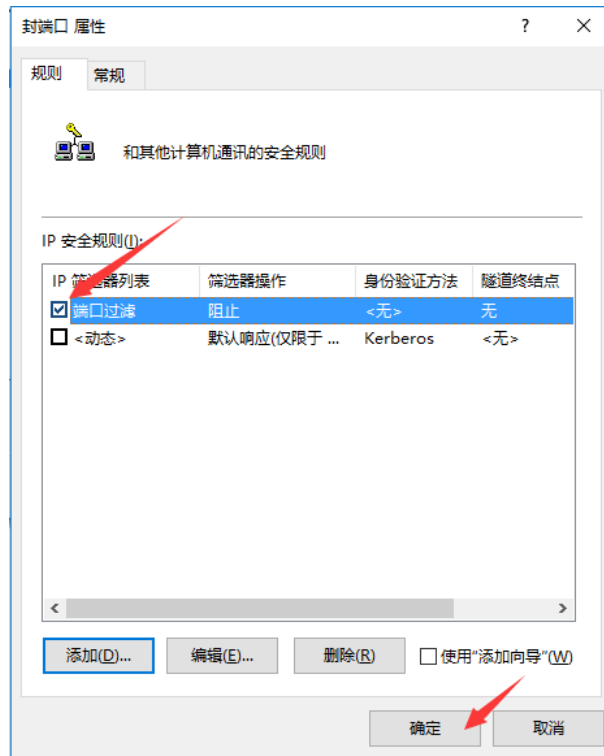
2. 选择“常规”选项卡，给这个筛选器起名“阻止”，然后“确定”。

点击

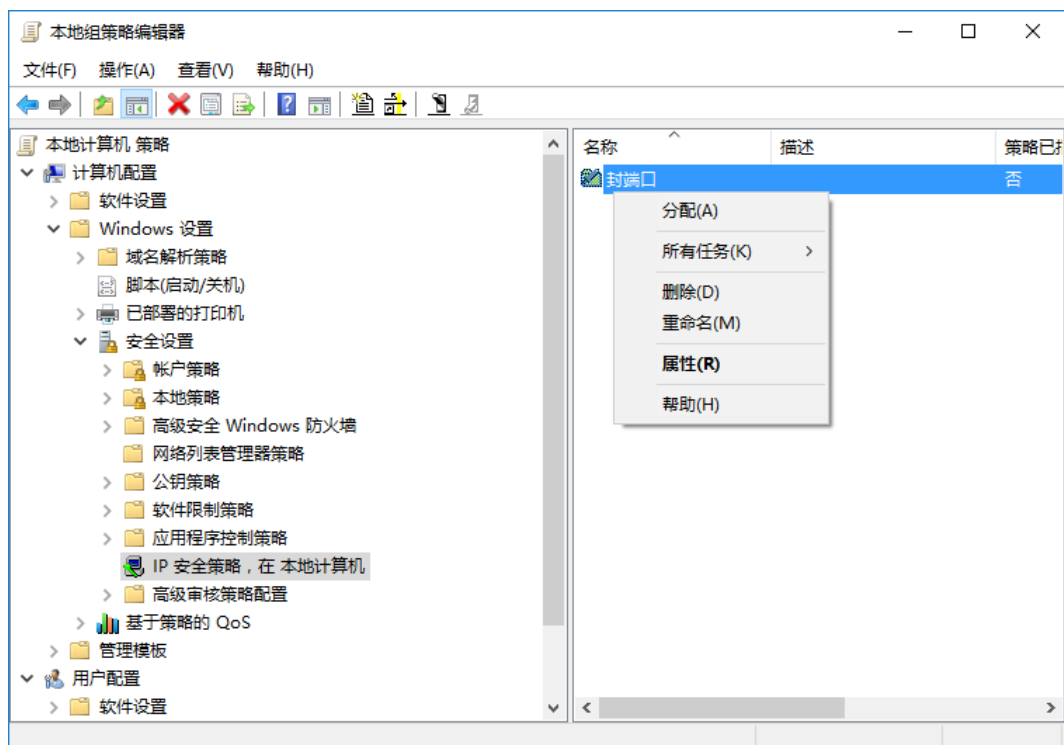
3. 确认“IP 筛选列表”选项卡下的“端口过滤”被选中。确认“筛选器操作”选项卡下的“阻止”被选中。然后点击“关闭”。



4. 确认安全规则配置正确。点击确定。



5. 在“组策略编辑器”上，右键“分配”，将规则启用。



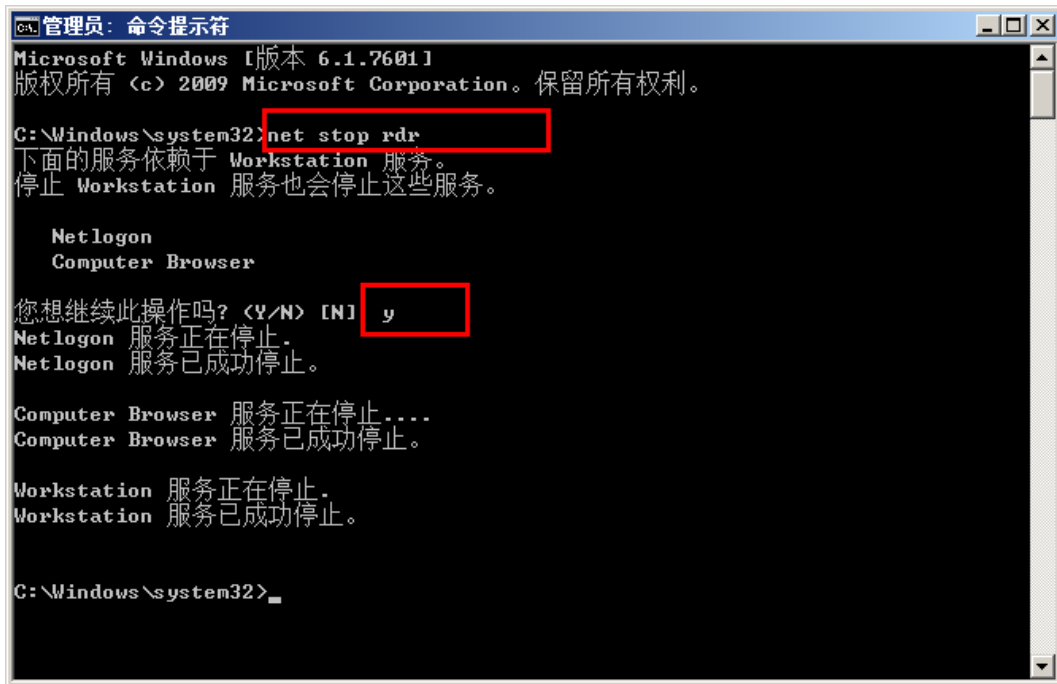
2.3 针对 WIN7 手工处置方式

2.3.1 方式一：命令行停止服务

依次点击“开始”-“所有程序”-“附件”，在“命令提示符”上点击鼠标右键，选择“以管理员身份运行（A）”



打开“管理员：命令提示符”窗口，输入“net stop rdr”回车，在“您想继续此操作吗？”处输入“Y”。



```
管理员: 命令提示符
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>net stop rdr
下面的服务依赖于 Workstation 服务。
停止 Workstation 服务也会停止这些服务。

Netlogon
Computer Browser

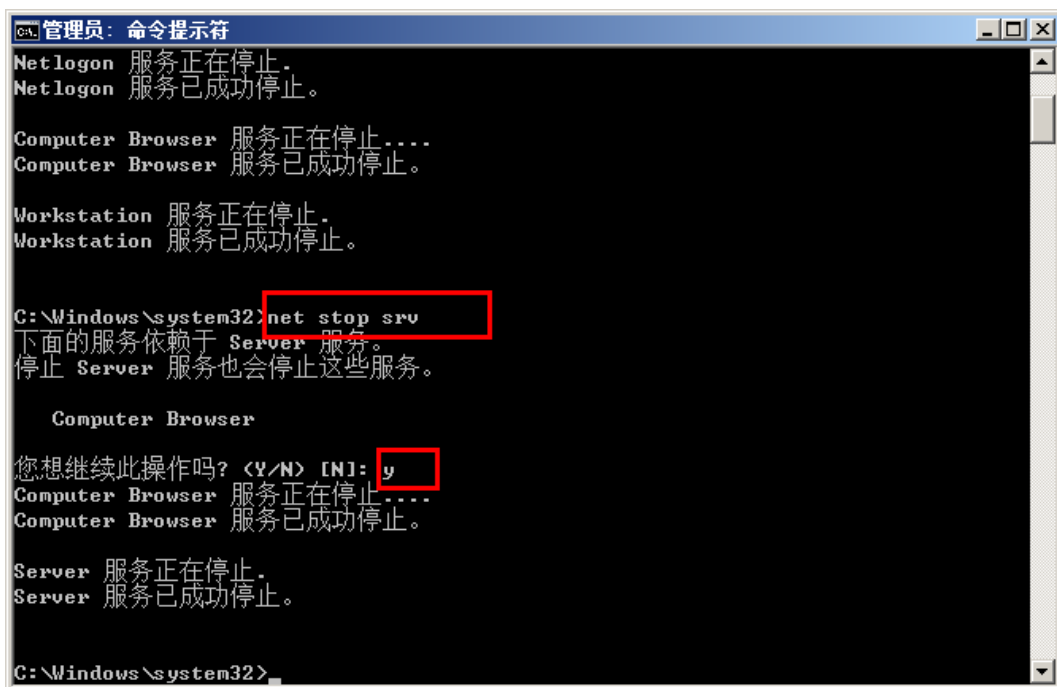
您想继续此操作吗? <Y/N> [N] y
Netlogon 服务正在停止。
Netlogon 服务已成功停止。

Computer Browser 服务正在停止....
Computer Browser 服务已成功停止。

Workstation 服务正在停止。
Workstation 服务已成功停止。

C:\Windows\system32>
```

输入“net stop srv”回车，在“您想继续此操作吗？”处输入”Y”。



```
管理员: 命令提示符
Netlogon 服务正在停止。
Netlogon 服务已成功停止。

Computer Browser 服务正在停止....
Computer Browser 服务已成功停止。

Workstation 服务正在停止。
Workstation 服务已成功停止。

C:\Windows\system32>net stop srv
下面的服务依赖于 Server 服务。
停止 Server 服务也会停止这些服务。

Computer Browser

您想继续此操作吗? <Y/N> [N]: y
Computer Browser 服务正在停止....
Computer Browser 服务已成功停止。

Server 服务正在停止。
Server 服务已成功停止。

C:\Windows\system32>
```

输入“net stop netbt”回车，在“您想继续此操作吗？”处输入”Y”。


```
管理员: 命令提示符
Computer Browser
您想继续此操作吗? <Y/N> [N]: y
Computer Browser 服务正在停止....
Computer Browser 服务已成功停止。

Server 服务正在停止。
Server 服务已成功停止。

C:\Windows\system32>net stop netbt
下面的服务依赖于 NetBT 服务。
停止 NetBT 服务也会停止这些服务。

TCP/IP NetBIOS Helper
您想继续此操作吗? <Y/N> [N]: y
TCP/IP NetBIOS Helper 服务正在停止。
TCP/IP NetBIOS Helper 服务已成功停止。

NetBT 服务正在停止.....
NetBT 服务无法停止。

C:\Windows\system32>
```

完成服务的停用。

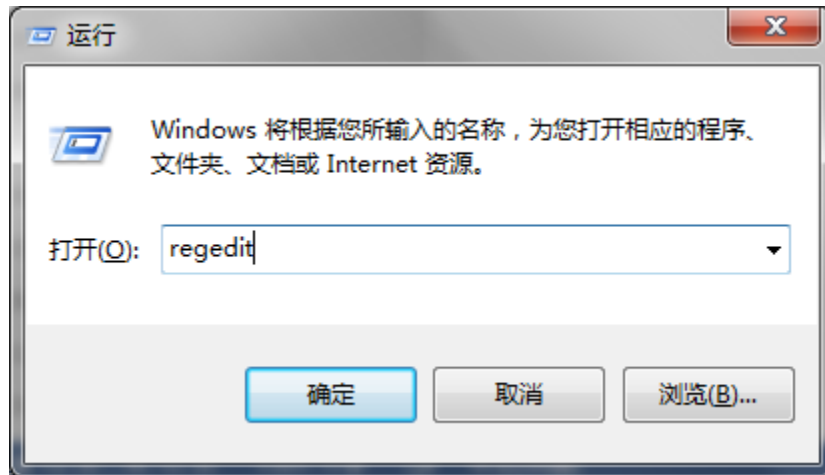
查看网络连接状态情况。

```
管理员: C:\Windows\System32\cmd.exe

C:\Windows\system32>netstat -an | more
```

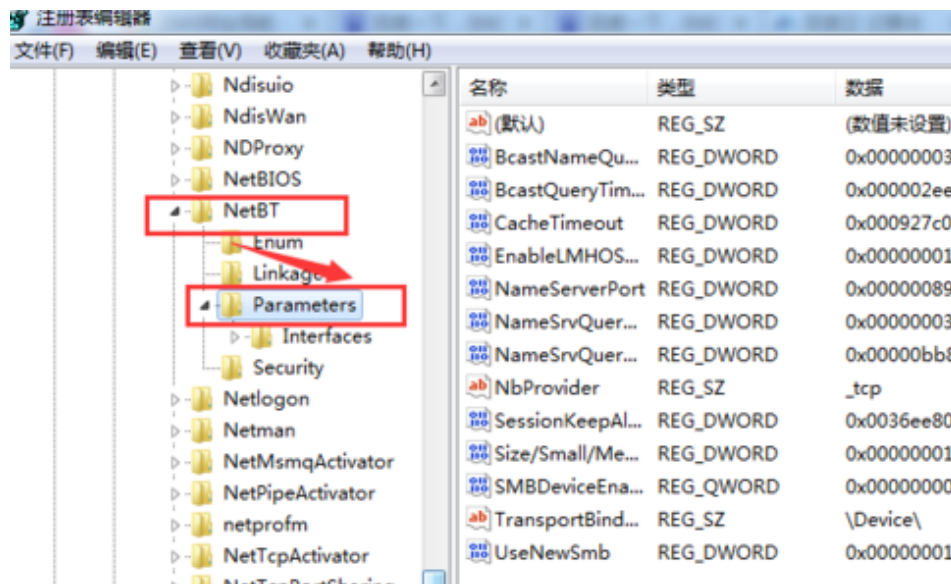
2.3.2 方式二：修改注册表

点击“开始”找到“所有程序”中的“附件”中的“运行”程序，然后在运行框中输入“regedit”然后点击确定按钮

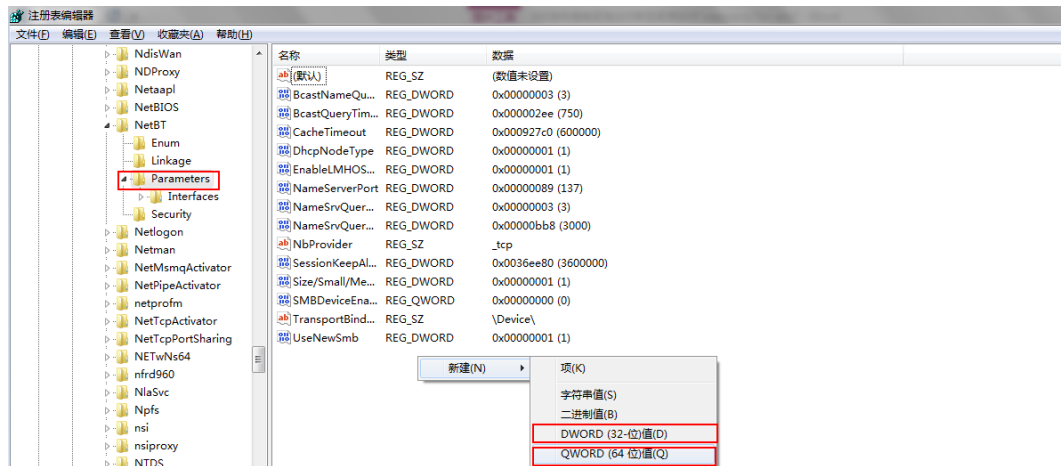


依次点击注册表选项”

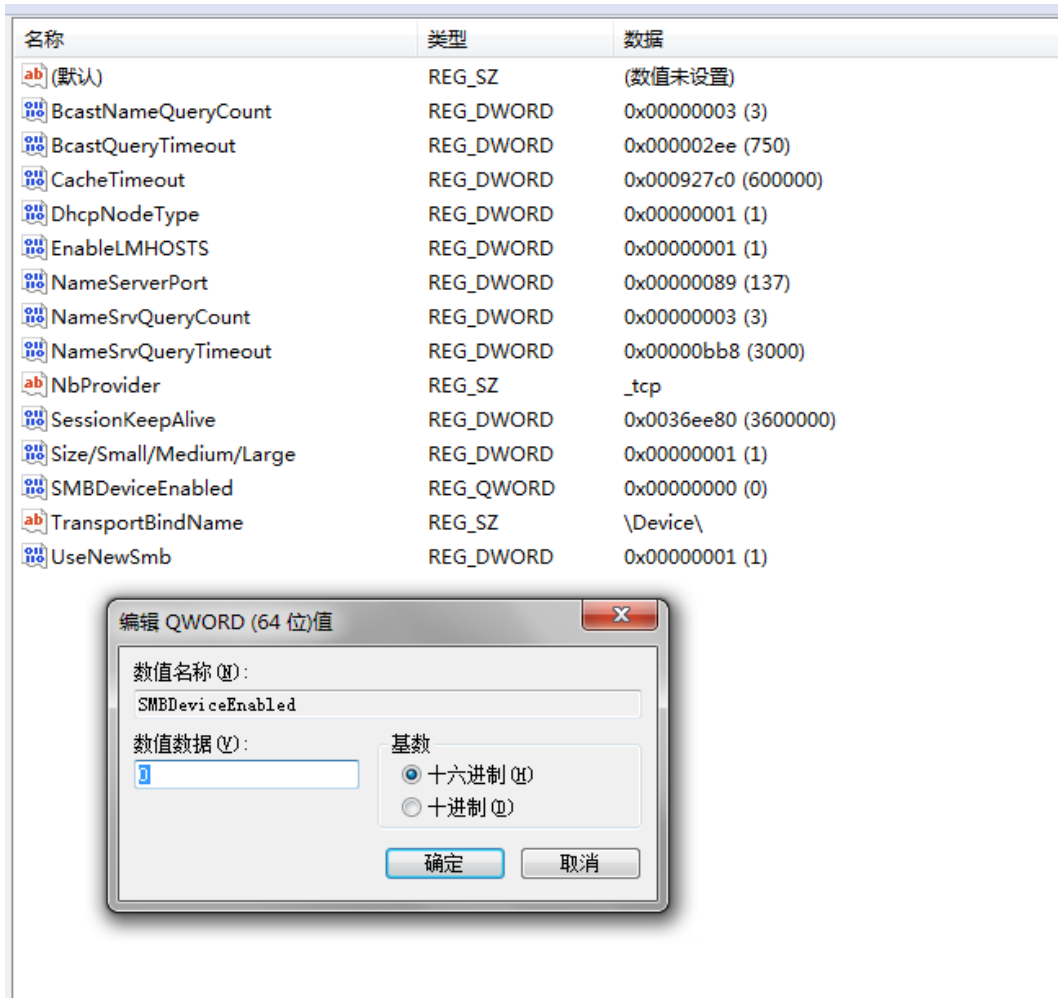
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters “，进入 NetBT 这个服务的相关注册表项



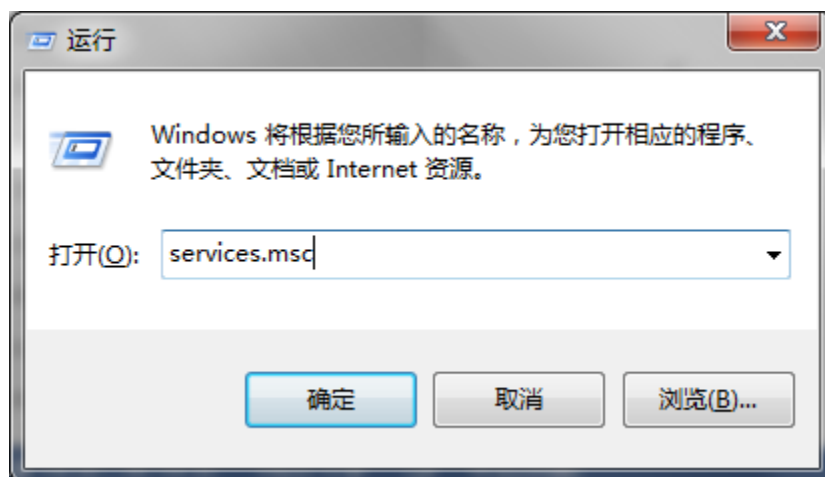
然后，在 Parameters 这个子项的右侧，点击鼠标右键，“新建”，“QWORD（64 位）值”（32 位操作系统选择 32 位值），然后重命名为“SMBDeviceEnabled”，再把这个子键的值改为 0



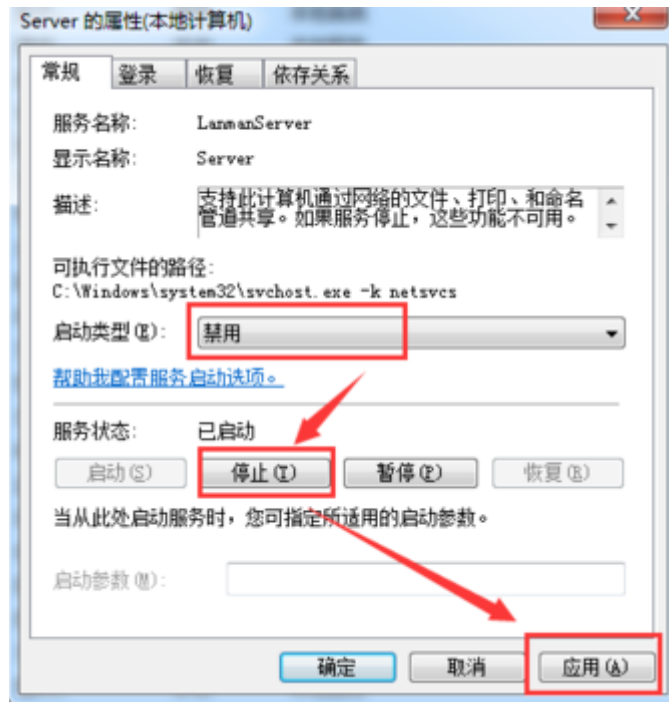
名称	类型	数据
(默认)	REG_SZ	(数值未设置)
BcastNameQueryCount	REG_DWORD	0x00000003 (3)
BcastQueryTimeout	REG_DWORD	0x000002ee (750)
CacheTimeout	REG_DWORD	0x000927c0 (600000)
DhcpNodeType	REG_DWORD	0x00000001 (1)
EnableLMHOSTS	REG_DWORD	0x00000001 (1)
NameServerPort	REG_DWORD	0x00000089 (137)
NameSrvQueryCount	REG_DWORD	0x00000003 (3)
NameSrvQueryTimeout	REG_DWORD	0x00000bb8 (3000)
NbProvider	REG_SZ	_tcp
SessionKeepAlive	REG_DWORD	0x0036ee80 (3600000)
Size/Small/Medium/Large	REG_DWORD	0x00000001 (1)
SMBDeviceEnabled	REG_QWORD	0x00000000 (0)
TransportBindName	REG_SZ	\Device\
UseNewSmb	REG_DWORD	0x00000001 (1)



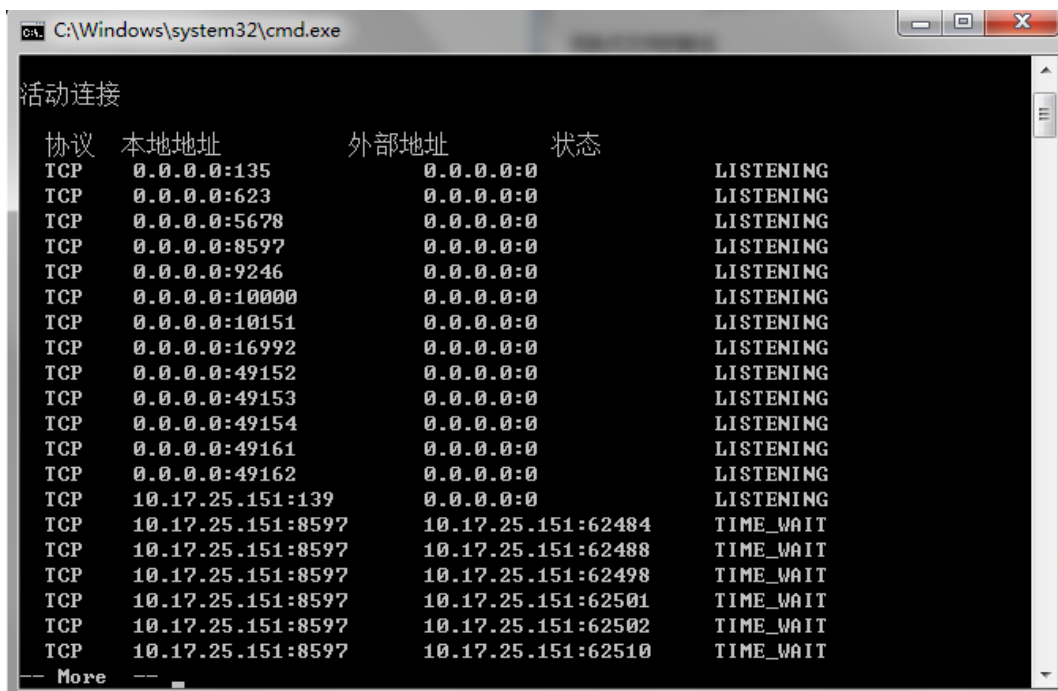
依次点击“开始”，“运行”，输入 services.msc，进入服务管理控制台



找到 server 服务，双击进入管理控制页面。把这个服务的启动类型更改为“禁用”，服务状态更改为“停止”，最后点击应用



最后一步重启系统后在命令行中输入“netstat -an|more”检查 445 端口是否已经成功关闭。



2.3.3 方式三：启用 windows 防火墙

在桌面右下角网络连接处点击右键，单击“打开网络和共享中心”，



在网络和共享中心，点击左下角“Windows 防火墙”字样，



打开“Windows 防火墙”管理界面，在左侧功能区点击“打开或关闭 Windows 防火墙”，



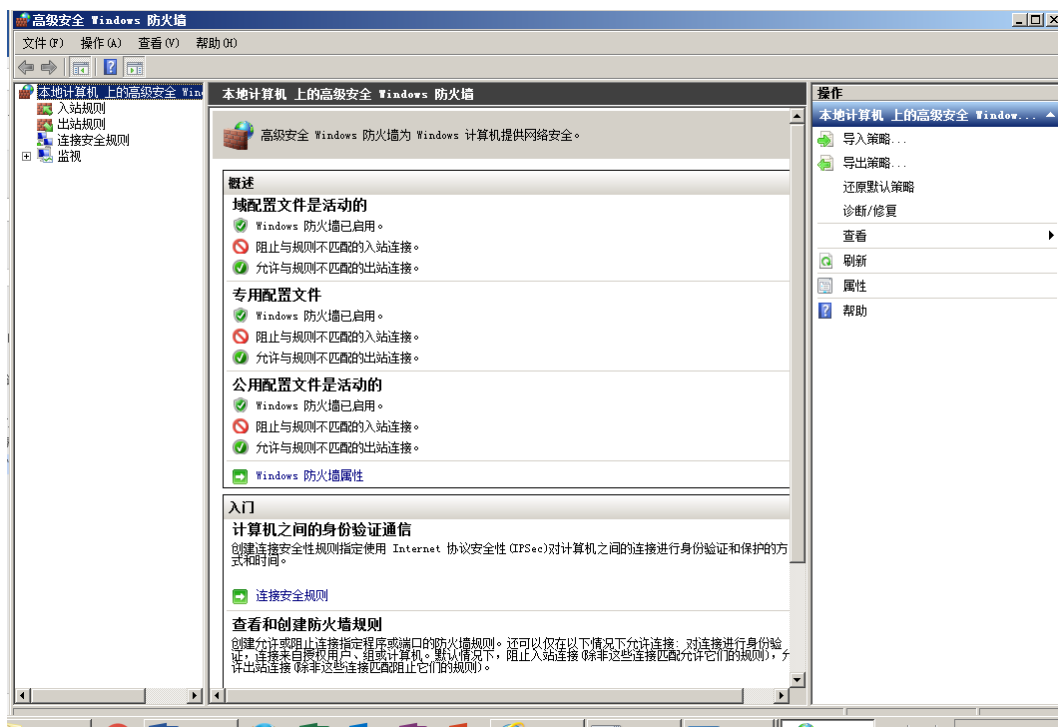
打开“自定义设置”界面，分别点击下图中红框内“启用 Windows 防火墙”，然后点击“确定”，回到“Windows 防火墙”窗口。



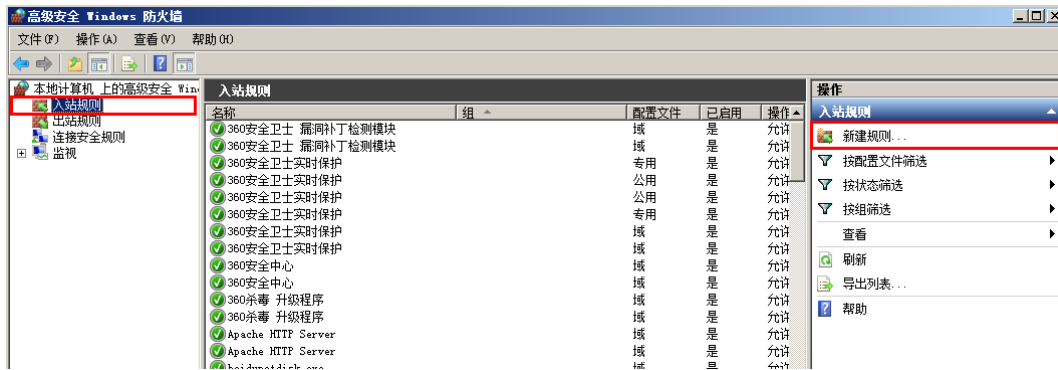
在左侧功能区点击“高级设置”字样，



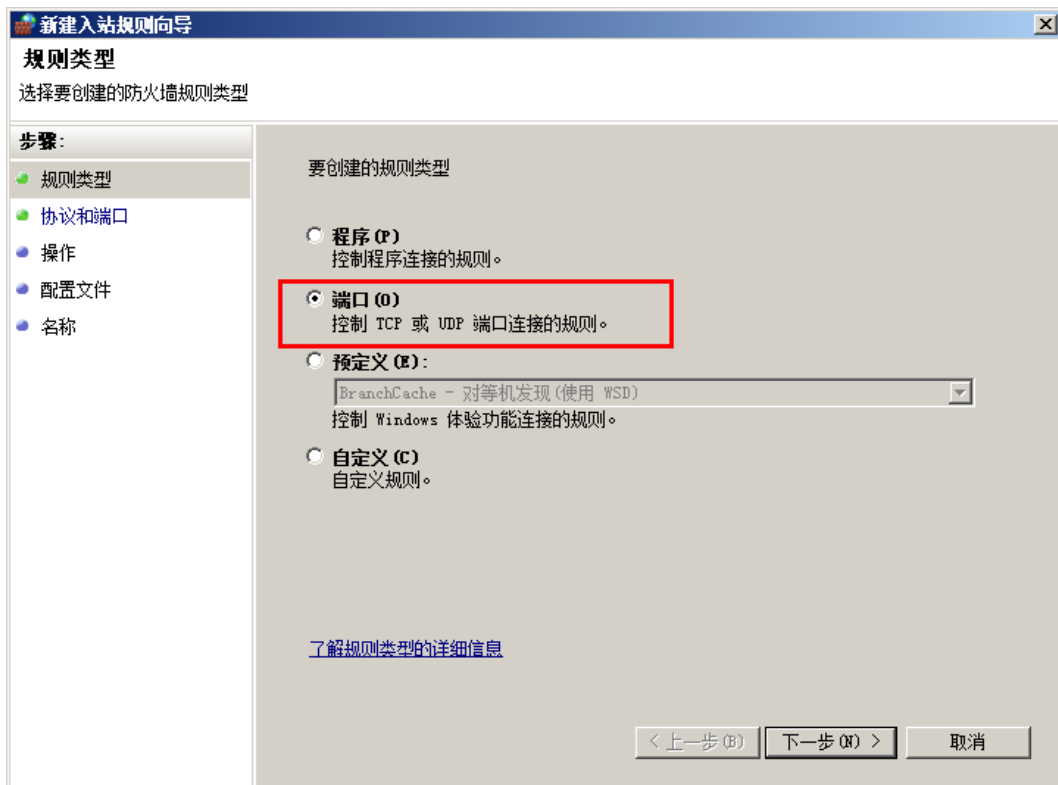
打开“高级安全 Windows 防火墙”窗口，



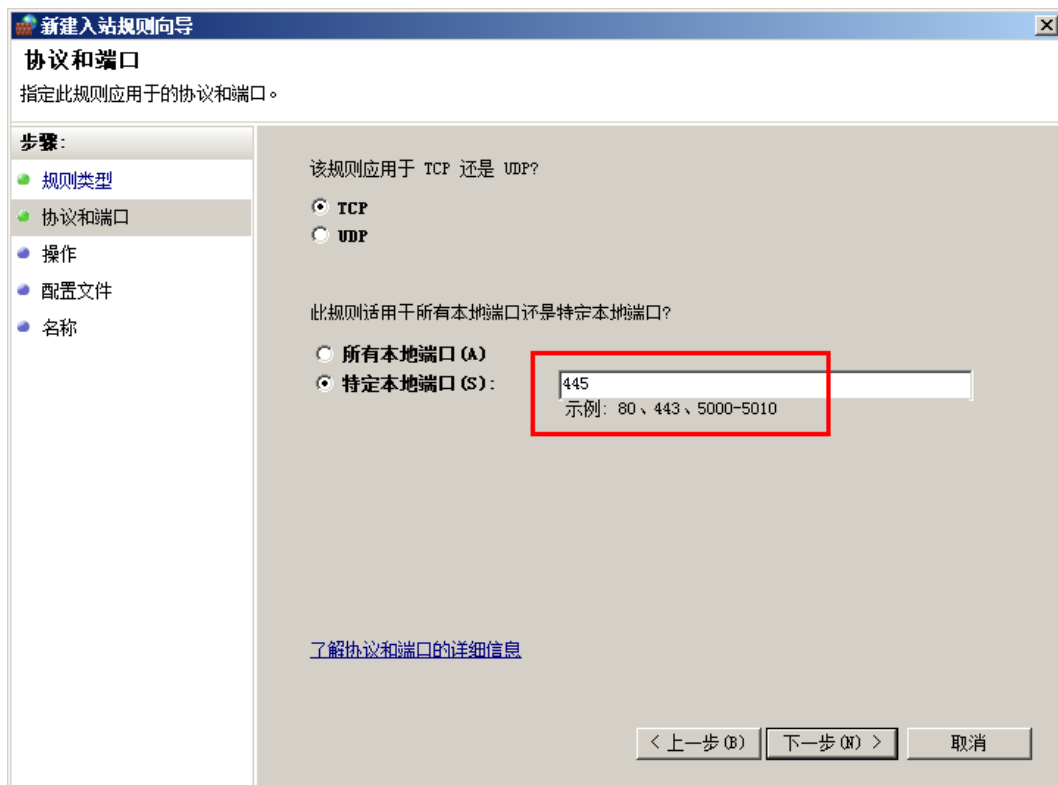
点击“入站规则”-“新建规则”，



打开“新建入站规则向导”界面，在规则类型页，选择“端口（0）”，然后点击“下一步”，



在协议和端口页，特定本地端口处，输入“445”，然后点击“下一步”，



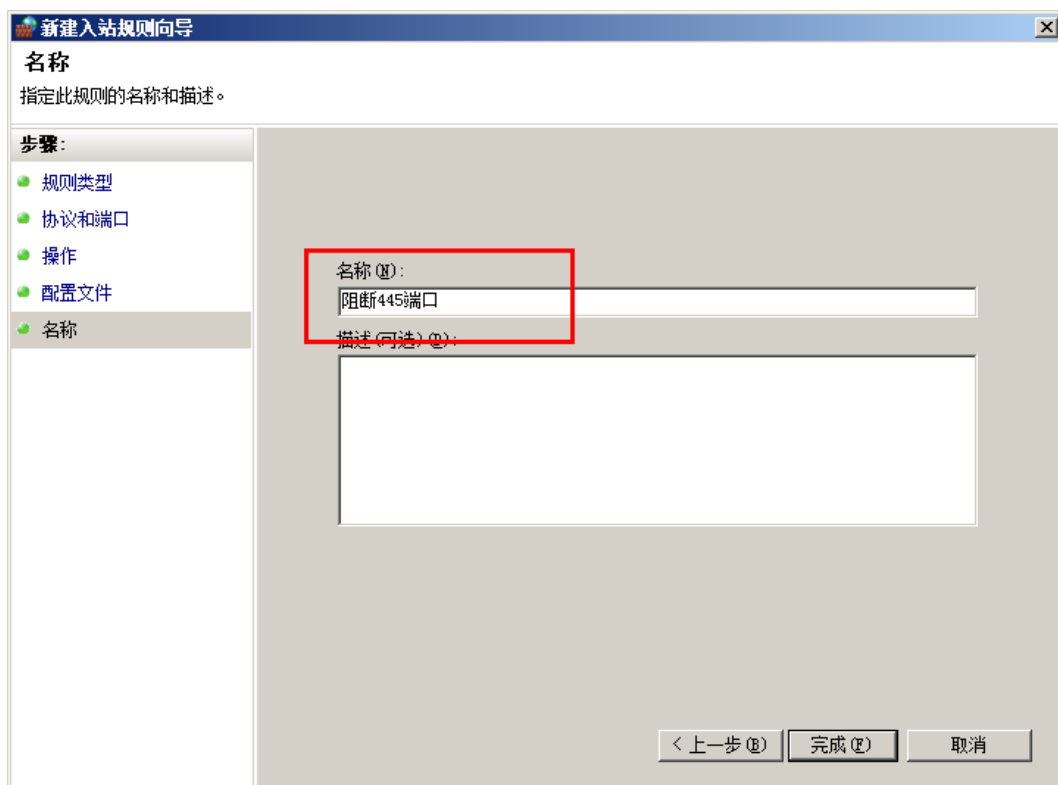
在操作页，选中“阻止连接”，然后点击下一步，



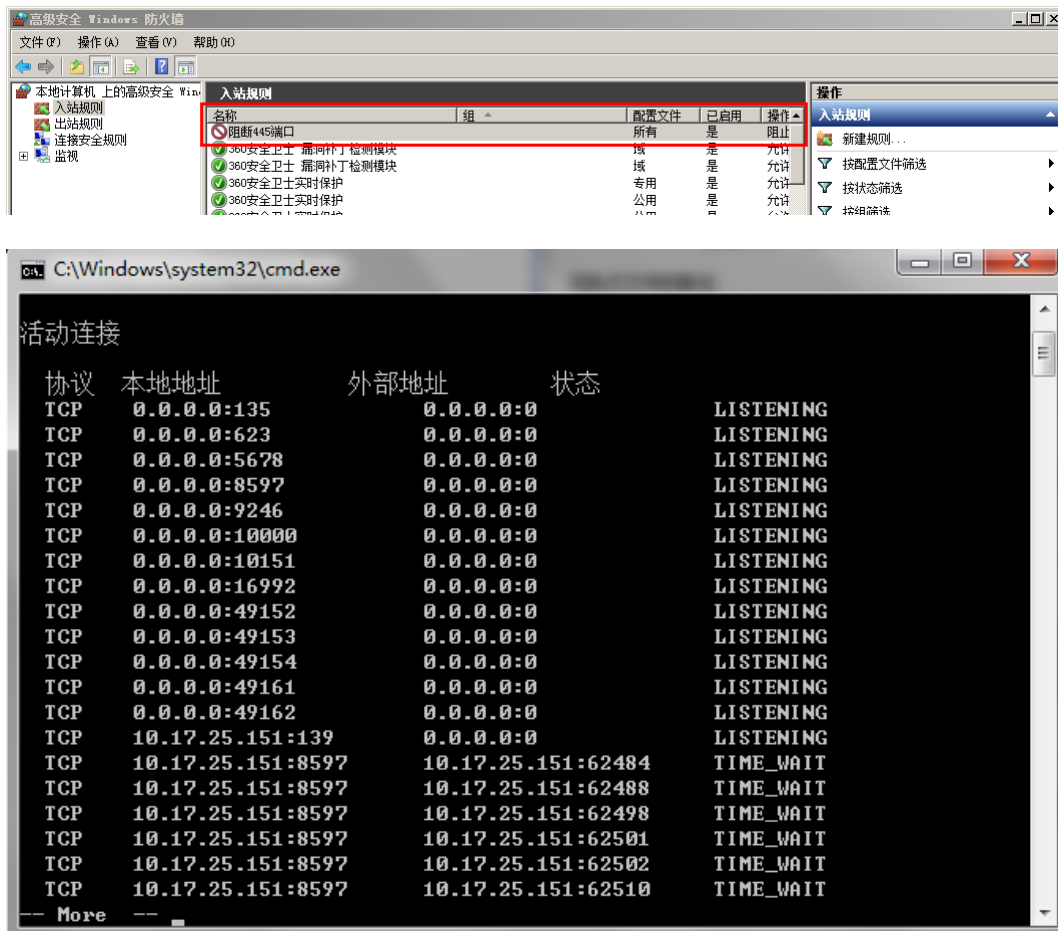
在配置文件页，“何时应用该规则？”处全部选中，然后点击下一步，



打开“名称”页，在名称处输入“阻断 445 端口”，然后点击“完成”。



此时可以看到入站规则最顶端出现刚添加的“阻断 445”规则，配置完成。



3 核心网络设备应急处置操作指南

大型机构由于设备众多，为了避免感染设备之后的广泛传播，建议利用各网络设备的 ACL 策略配置，以实现临时封堵。

该蠕虫病毒主要利用 TCP 的 139、445 端口进行传播，对于各大企事业单位影响很大。为了阻断病毒快速传播，建议在核心网络设备的三层接口位置，配置 ACL 规则从网络层面阻断 TCP 139、445 端口的通讯。

以下内容是基于较为流行的网络设备，举例说明如何配置 ACL 规则，以禁止 TCP 139、445 网络端口传输，仅供大家参考。在实际操作中，请协调网络管理人员或网络设备厂商服务人员，根据实际网络环境在核心网络设备上配置。

3.1 Juniper 设备的建议配置（示例）

```
set firewall family inet filter deny-wannacry term deny445 from protocol tcp
```

```
set firewall family inet filter deny-wannacry term deny445 from destination-  
port 445
```

```
set firewall family inet filter deny-wannacry term deny445 from destination-  
port 139
```

```
set firewall family inet filter deny-wannacry term deny445 then discard  
set firewall family inet filter deny-wannacry term default then accept
```

#在全局应用规则

```
set forwarding-options family inet filter output deny-wannacry  
set forwarding-options family inet filter input deny-wannacry
```

#在三层接口应用规则

```
set interfaces [需要挂载的三层端口名称] unit 0 family inet filter output deny-  
wannacry
```

```
set interfaces [需要挂载的三层端口名称] unit 0 family inet filter input deny-  
wannacry
```

3.2 华三(H3C)设备的建议配置（示例）

新版本：

```
acl number 3050
```

```
rule deny tcp destination-port 445
```

```
rule deny tcp destination-port 139
```

```
rule permit ip
```

```
interface [需要挂载的三层端口名称]
```

```
packet-filter 3050 inbound
```

packet-filter 3050 outbound

旧版本:

acl number 3050

rule permit tcp destination-port 445

rule permit tcp destination-port 139

traffic classifier deny-wannacry

if-match acl 3050

traffic behavior deny-wannacry

filter deny

qos policy deny-wannacry

classifier deny-wannacry behavior deny-wannacry

#在全局应用

qos apply policy deny-wannacry global inbound

qos apply policy deny-wannacry global outbound

#在三层接口应用规则

interface [需要挂载的三层端口名称]

qos apply policy deny-wannacry inbound

qos apply policy deny-wannacry outbound

3.3 华为设备的建议配置（示例）

acl number 3050

rule deny tcp destination-port eq 445

rule deny tcp destination-port eq 139

rule permit ip

traffic classifier deny-wannacry type and

if-match acl 3050

traffic behavior deny-wannacry

traffic policy deny-wannacry

classifier deny-wannacry behavior deny-wannacry precedence 5

interface [需要挂载的三层端口名称]

traffic-policy deny-wannacry inbound

traffic-policy deny-wannacry outbound

3.4 Cisco 设备的建议配置（示例）

旧版本：

```
ip access-list extended deny-wannacry
deny tcp any any eq 445
deny tcp any any eq 139
permit ip any any
```

interface [需要挂载的三层端口名称]

```
ip access-group deny-wannacry in
ip access-group deny-wannacry out
```

新版本：

```
ip access-list deny-wannacry
deny tcp any any eq 445
deny tcp any any eq 139
permit ip any any
```

interface [需要挂载的三层端口名称]

```
ip access-group deny-wannacry in
ip access-group deny-wannacry out
```

3.5 锐捷设备的建议配置（示例）

```
ip access-list extended deny-wannacry
deny tcp any any eq 445
```



```
deny tcp any any eq 139
```

```
permit ip any any
```

```
interface [需要挂载的三层端口名称]
```

```
ip access-group deny-wannacry in
```

```
ip access-group deny-wannacry out
```

4 互联网主机应急处置操作指南

采用快速处置方式，建议使用 360 安全卫士的“NSA 武器库免疫工具”，可一键检测修复漏洞、关闭高风险服务，包括精准检测出 NSA 武器库使用的漏洞是否已经修复，并提示用户安装相应的补丁。针对 Windows XP、Windows 2003 等无补丁的系统版本用户，防御工具能够帮助用户关闭存在高危风险的服务，从而对 NSA 黑客武器攻击的系统漏洞彻底“免疫”。

NSA 武器库免疫工具下载地址：<http://dl.360safe.com/nsa/nsatool.exe>



① 经检测，发现您的电脑存在该漏洞，请立即修复！

- | | |
|--------------------------|--------------------------|
| • EternalBlue (永恒之蓝) | • ErraticGopher (古怪地鼠) |
| • EternalChampion (永恒王者) | • EskimoRoll (爱斯基摩卷) |
| • EternalRomance (永恒浪漫) | • EducatedScholar (文雅学者) |
| • EternalSynergy (永恒协作) | • EclipsedWing (日食之翼) |
| • EmeraldThread (翡翠纤维) | • EsteemAudit(尊重审查) |

立即修复

通过360安全卫士安装补丁

