

360 企业安全针对“永恒之蓝”攻击紧急应对手册

目录

第一部分——通用环境指导	3
一、确认主机是否被感染	3
二、网络层面	4
1. 网络层 ACL 调整	4
2. IPS 特征库更新	9
三、服务器层面	9
1. 安装漏洞补丁	9
2. 免疫工具	10
3. 关闭服务	10
4. 组策略调整	13
四、终端层面	25
1. 免疫工具	25
2. 关闭服务	25
3. 组策略调整	28
4. 安装漏洞补丁	40
五、周一开机及上线保障指南	40
第二部分——针对已使用 360 企业安全产品的运维人员	42
第三部分——互联网主机应急处置操作指南	42

本手册分三部分对此次“永恒之蓝”攻击提供针对性防护建议：通用环境指导，360 企业安全产品操作指导，互联网主机防护指导。

第一部分——通用环境指导

此部分针对通用 IT 环境，从已感染主机的处理，到网络、服务器、终端几个层面的防护提供建议，应对此次攻击。最后提供了“周一开机及上线保障指南”，供 IT 管理员参考。

一、确认主机是否被感染

被感染的机器屏幕会显示如下的告知付赎金的界面：



如果主机已被感染：

则将该主机隔离或断网（拔网线）。若文档尚未被全部加密，则应立即关机，使用 PE 盘引导进入 PE 系统后将尚未加密的文档备份转移避免损失的进一步扩大。若客户存在该主机备份，则启动备份恢复程序。执行恢复后的主机应参照未被感染主机的防护措施加固后再入网。

如果主机未被感染：

从以下几个层面实施防护。

二、网络层面

1. 网络层 ACL 调整

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 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 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 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。

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 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
```

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 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

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) 华为设备的建议配置 (示例) :

```
acl number 3050
```

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

```
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
```

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
```

```
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
```

```
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
```

5) 锐捷设备的建议配置 (示例) :

```
ip access-list extended deny-wannacry
```

```
deny tcp any any eq 445
```

```
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
```

2. IPS 特征库更新

多数 IPS 厂商为了应对此类攻击，会针对性的升级特征库。建议 IT 安全、运维人员及时关注厂商发布的信息，并升级特征库。

三、服务器层面

1. 安装漏洞补丁

微软针对本次事件，对支持的操作系统在安全公告 MS17-010 中已发布相应补丁修复，对于部分已停服的 Win XP、2003 也已紧急发布补丁 KB4012598 修复。请在所有服务器及终端安装依据操作系统类型不同对应安装相应的补丁。下载来源：

MS17-010 Security Update:

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

KB4012598

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>

or 360 云盘：

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

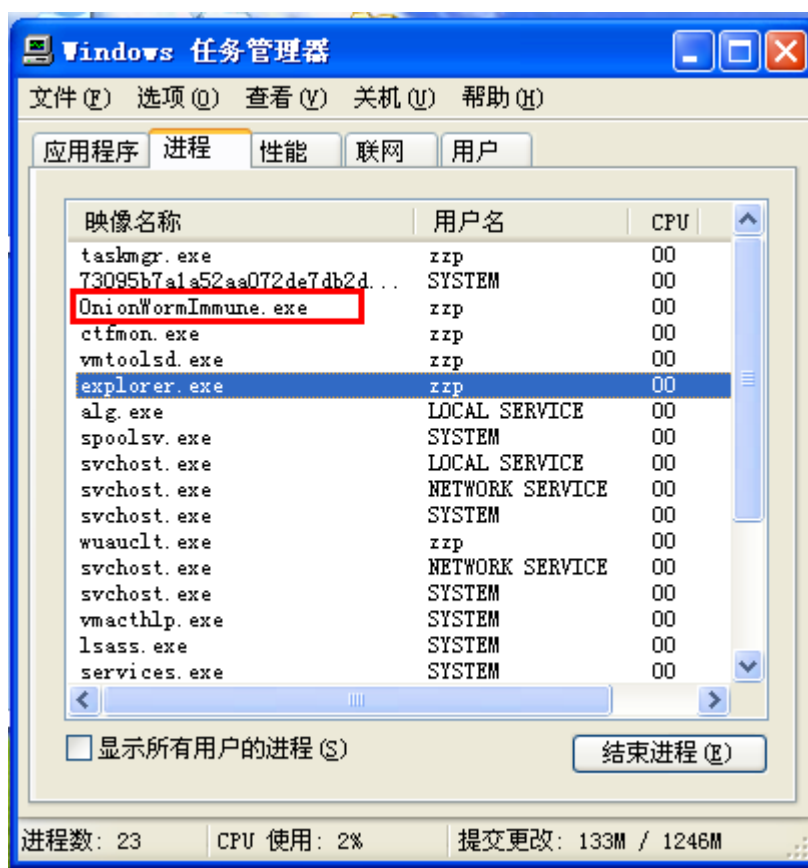
根据不用的操作系统版本，手动安装以上补丁后，可直接修复此次“永恒之蓝”攻击的所利用的系统漏洞。

另外也可更新天擎控制中心补丁库升级到 1.0.1.2825 及以上版本，并安装其中包含的所有高危漏洞。

打补丁可能会对用户的现有业务系统、办公软件等造成影响，在生产服务器上安装前，需做好兼容性测试，避免影响业务。

2. 免疫工具

在补丁安装完成前，为避免服务器感染，手工或使用主机管理系统下发免疫工具（下载页面：<http://b.360.cn/other/onionwormimmune>），免疫工具将不影响当前 445 端口业务的运行，运行后可在任务管理器中检查其状态：



3. 关闭服务

如果免疫工具运行遇到问题，也可选择关闭 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 sc config srv start= disabled (注意 disabled 前有空格)

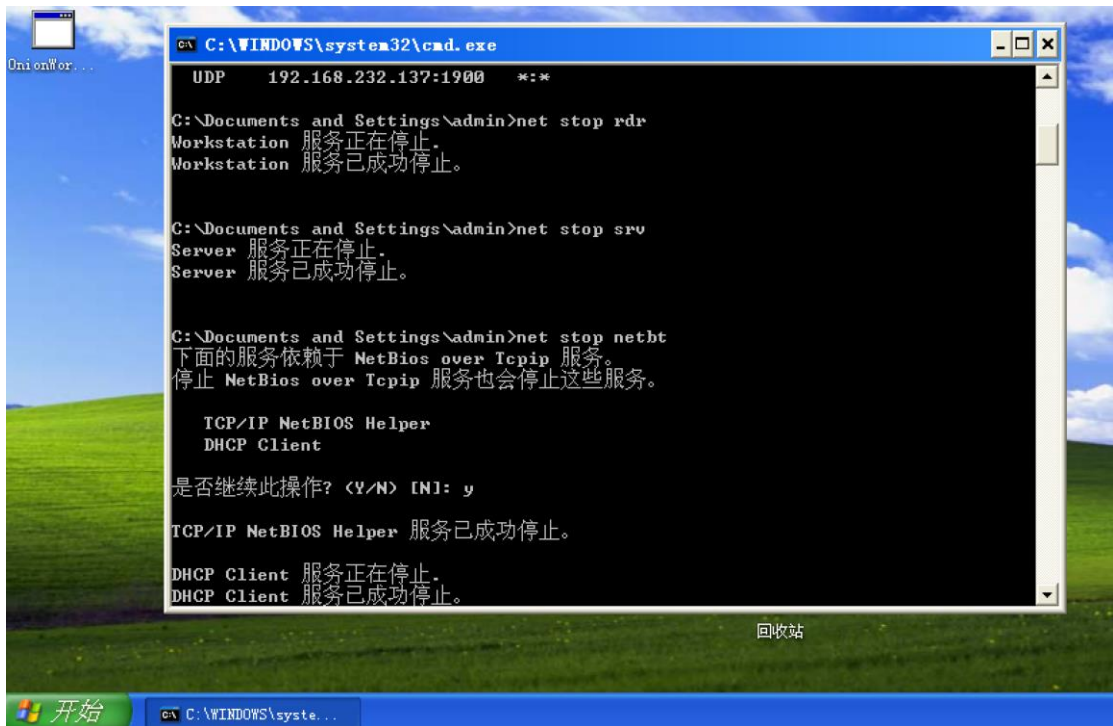
sc config netbt start= disabled (注意 disabled 前有空格)

输入 net stop rdr 回车

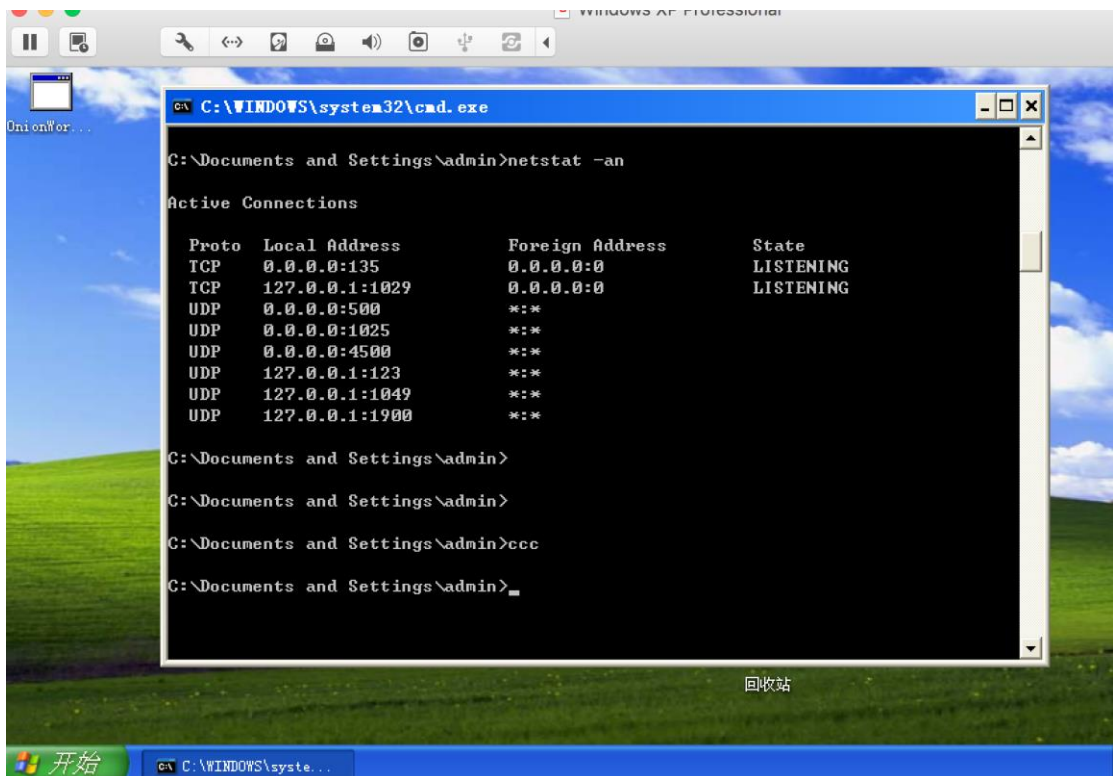
net stop srv 回车

net stop netbt 回车

如果有提问 “您想继续此操作吗? (Y/N) [N]:”，输入 Y



再次输入 netstat -an，成功关闭 445 端口。



4. 组策略调整

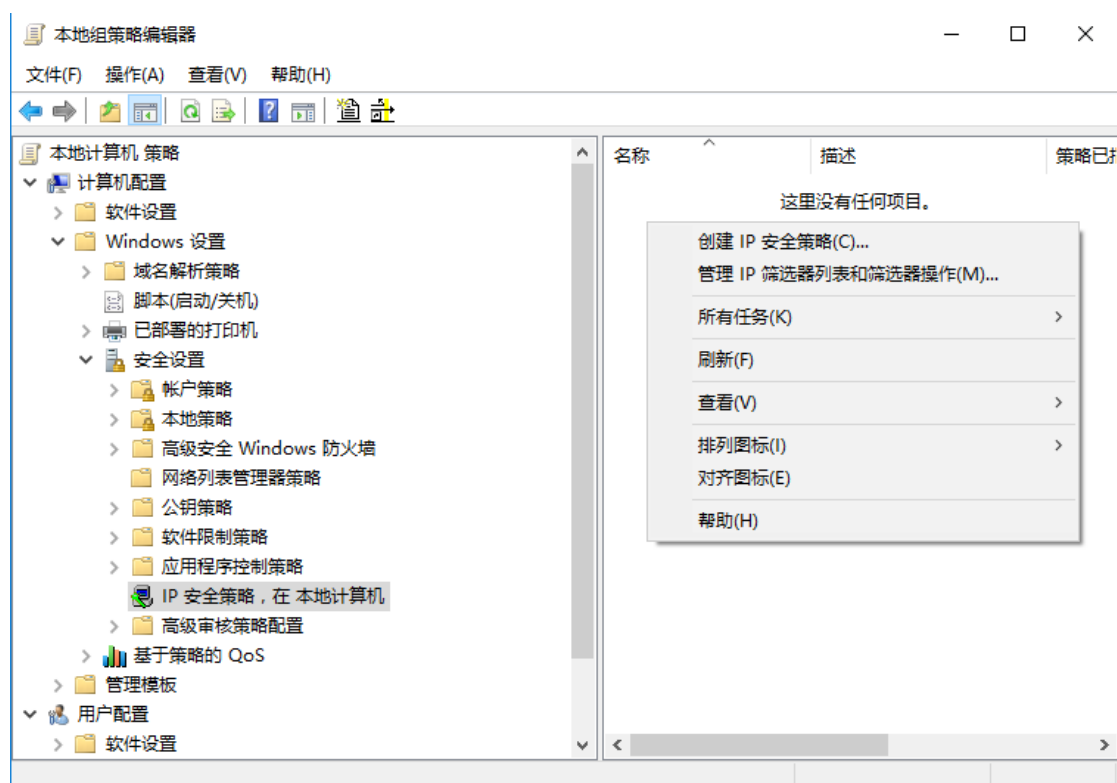
另一方式是用主机 ACL 策略封堵 445 端口。请注意，2、3、4 这三种方式，做到其中任意一个即可达到临时免疫的目的。

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，

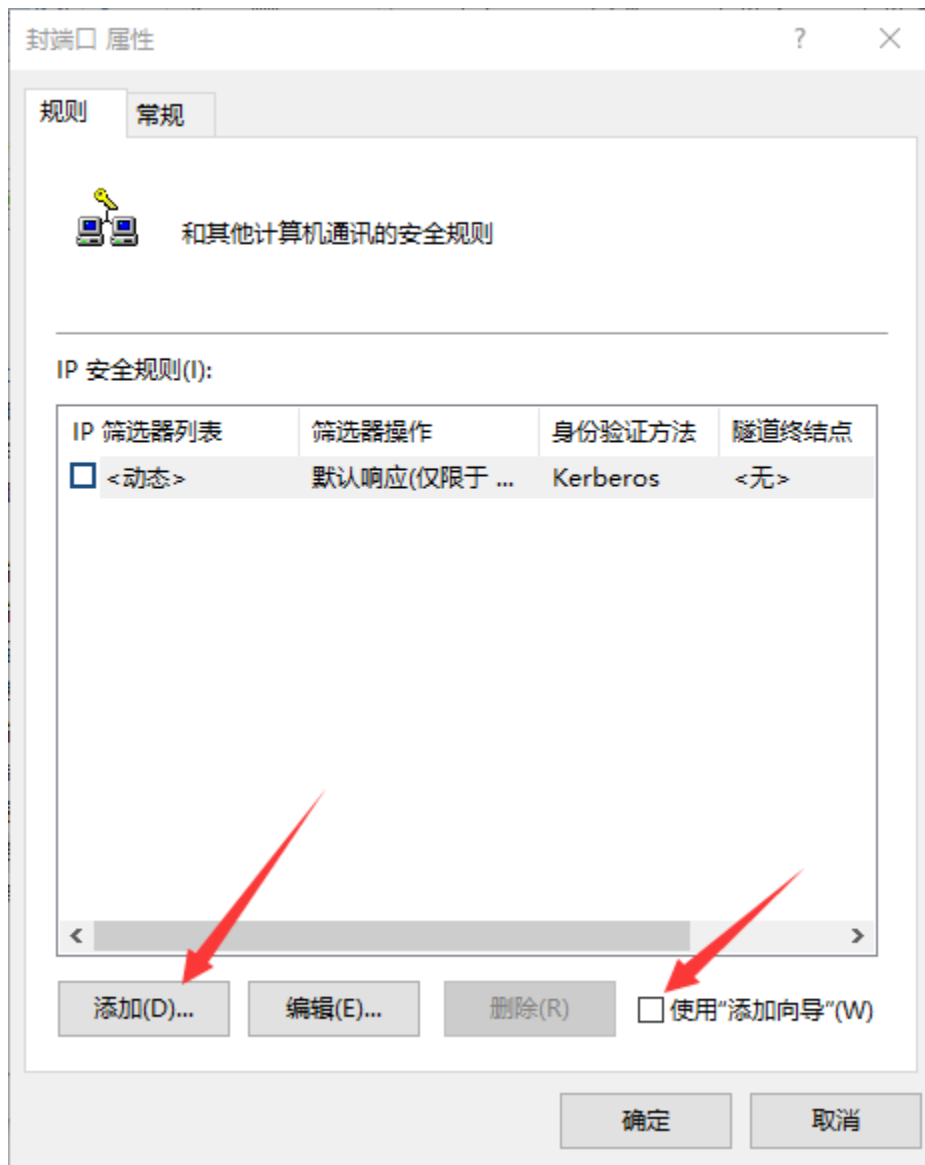
在编辑器右边空白处鼠标右键单击，选择“创建 IP 安全策略”



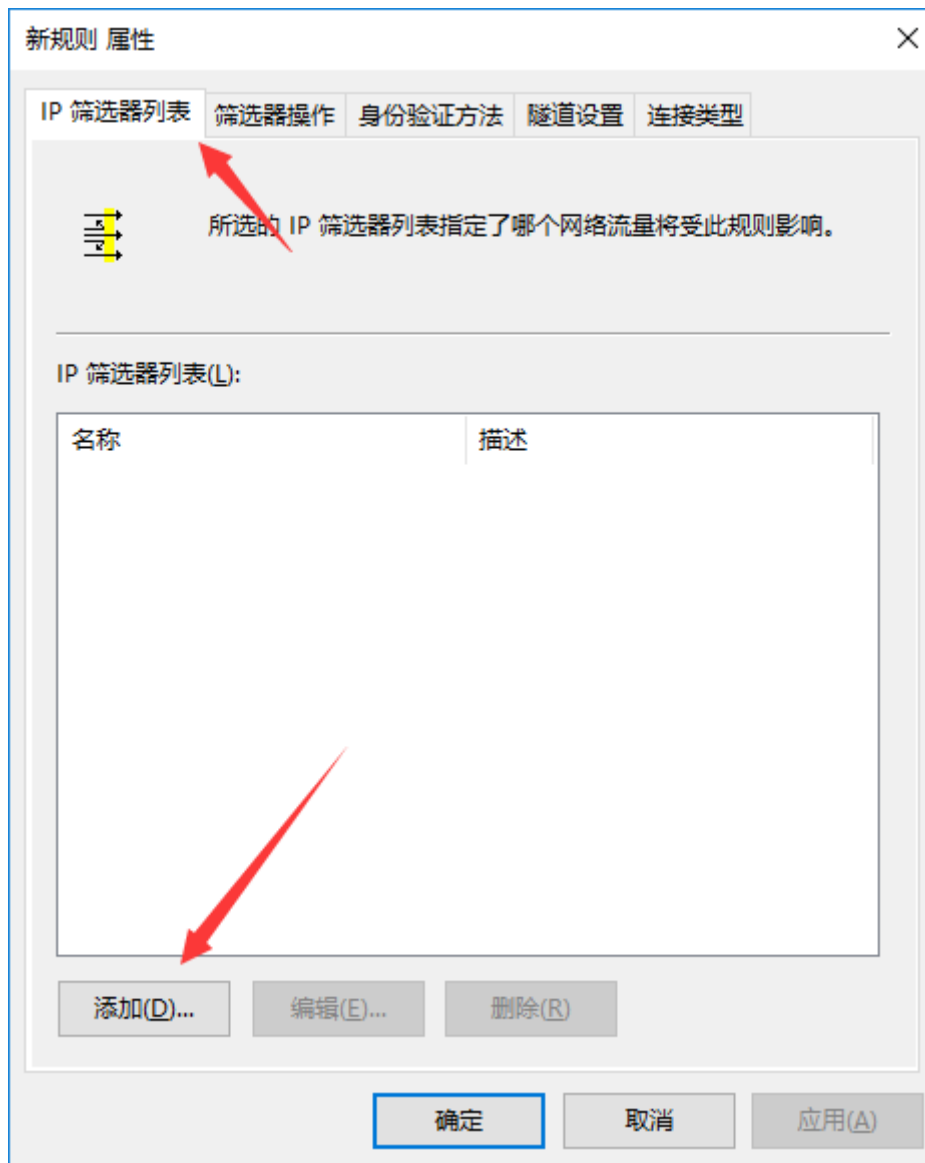
下一步->名称填写“封端口”，下一步->下一步->勾选编辑属性，并点完成



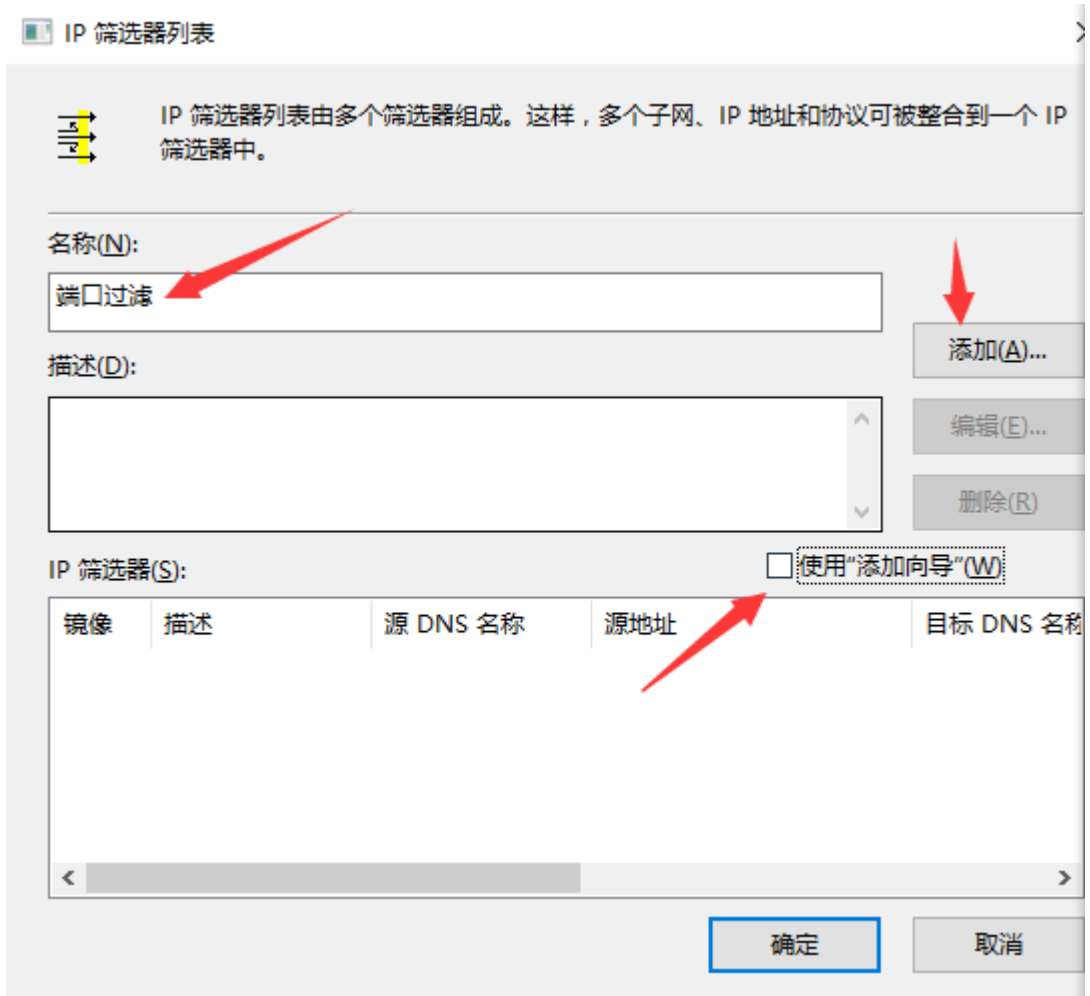
去掉“使用添加向导”的勾选后，点击“添加”



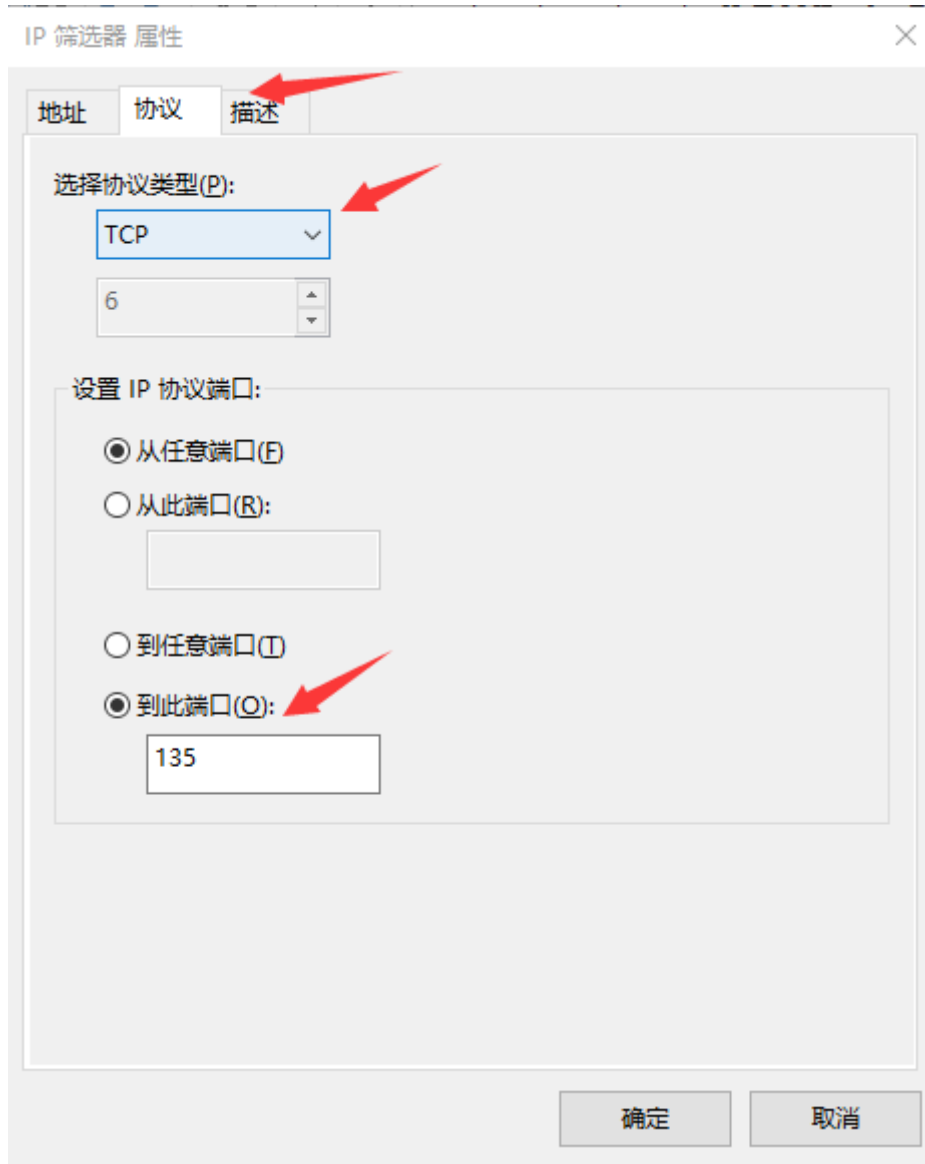
在新弹出的窗口，选择“IP 筛选列表”选项卡，点击“添加”



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”

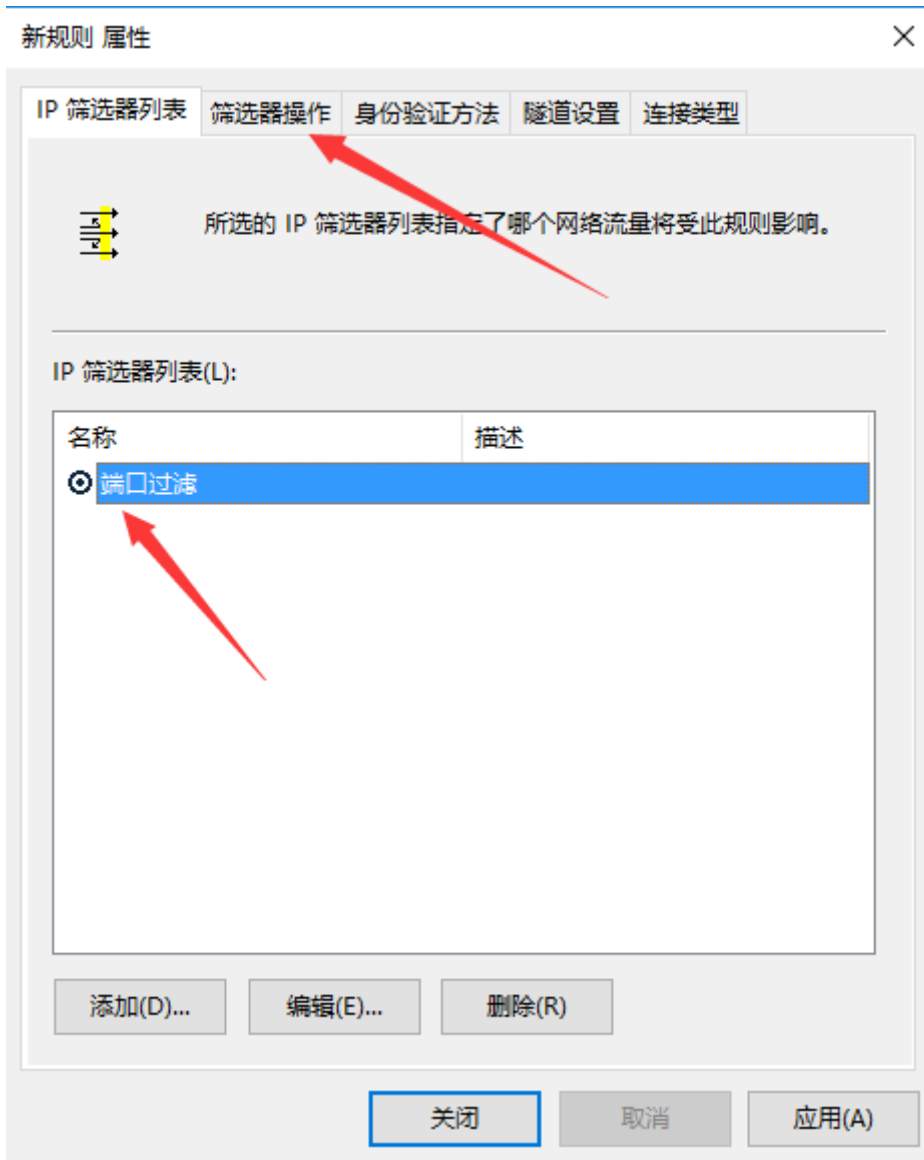


在新弹出的窗口中，“协议”选项卡下，选择协议和设置到达端口信息，并点确定。



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。

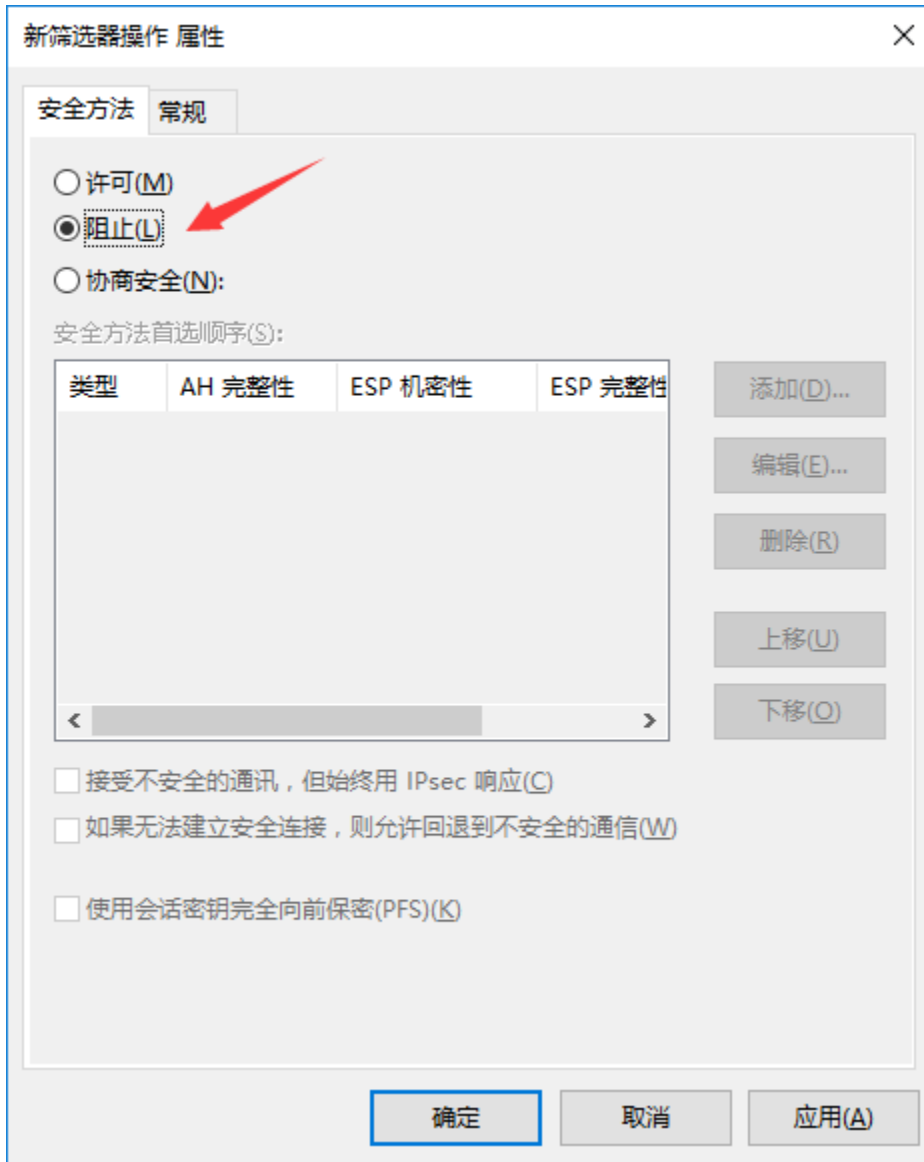
选中刚添加完成的“端口过滤”规则，然后选择“筛选器操作”选项卡。



去掉“使用添加向导”勾选，单击“添加”按钮



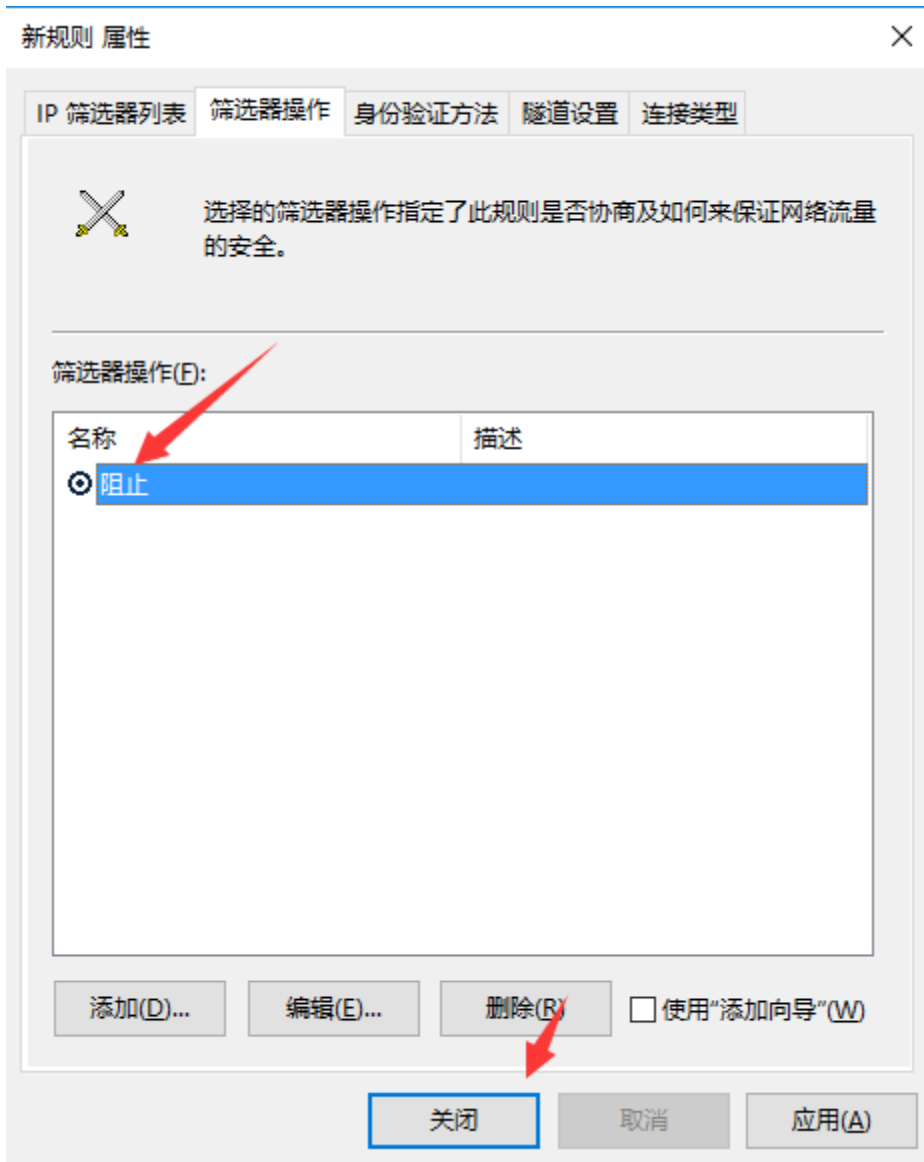
1. 选择“阻止”



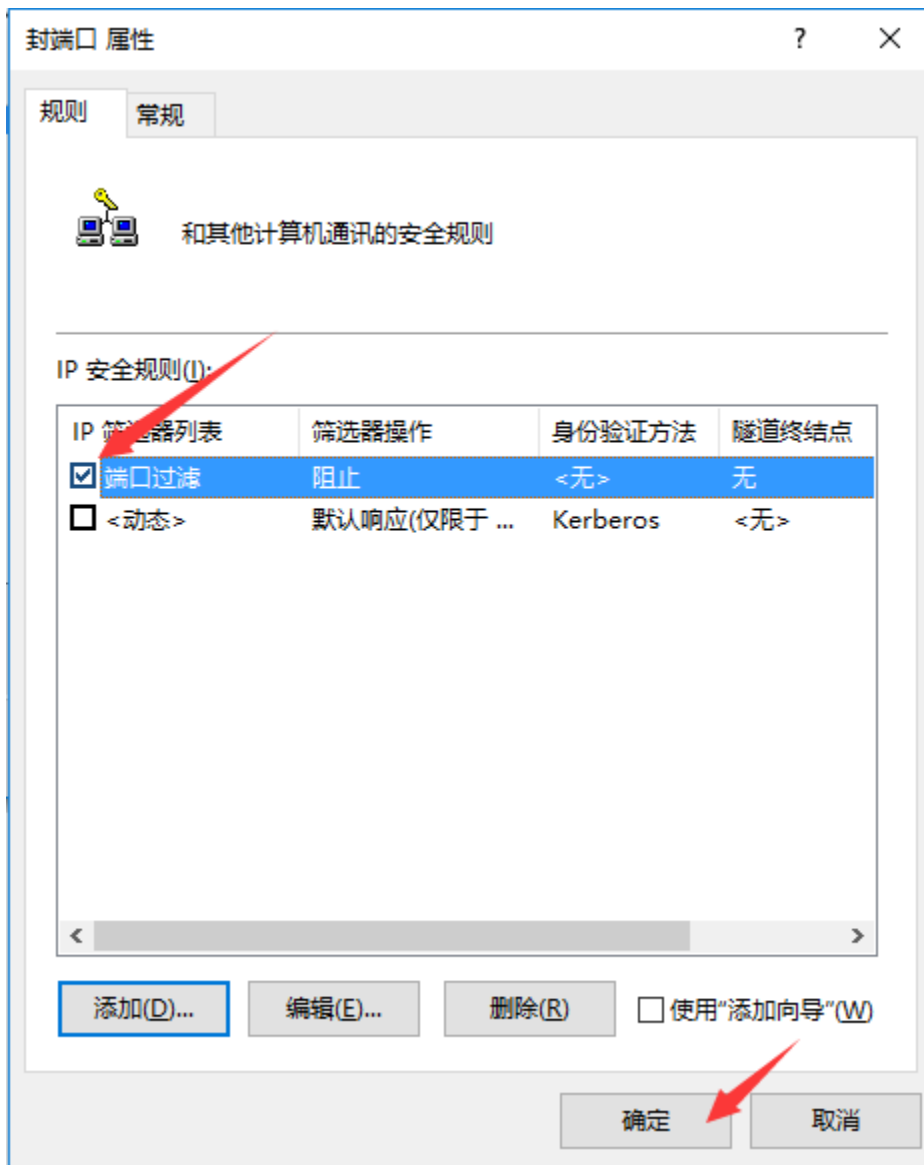
2. 选择“常规”选项卡，给这个筛选器起名“阻止”，然后“确定”。

点击

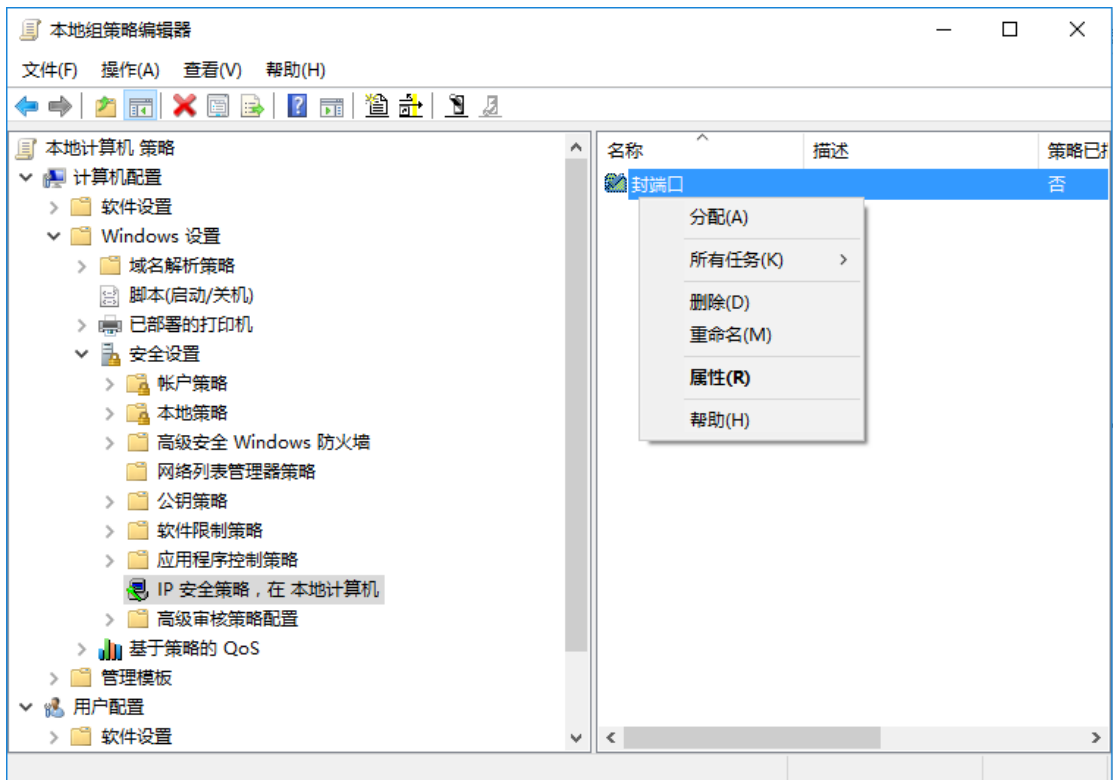
3. 确认“IP 筛选列表”选项卡下的“端口过滤”被选中。确认“筛选器操作”选项卡下的“阻止”被选中。然后点击“关闭”。



4. 确认安全规则配置正确。点击确定。



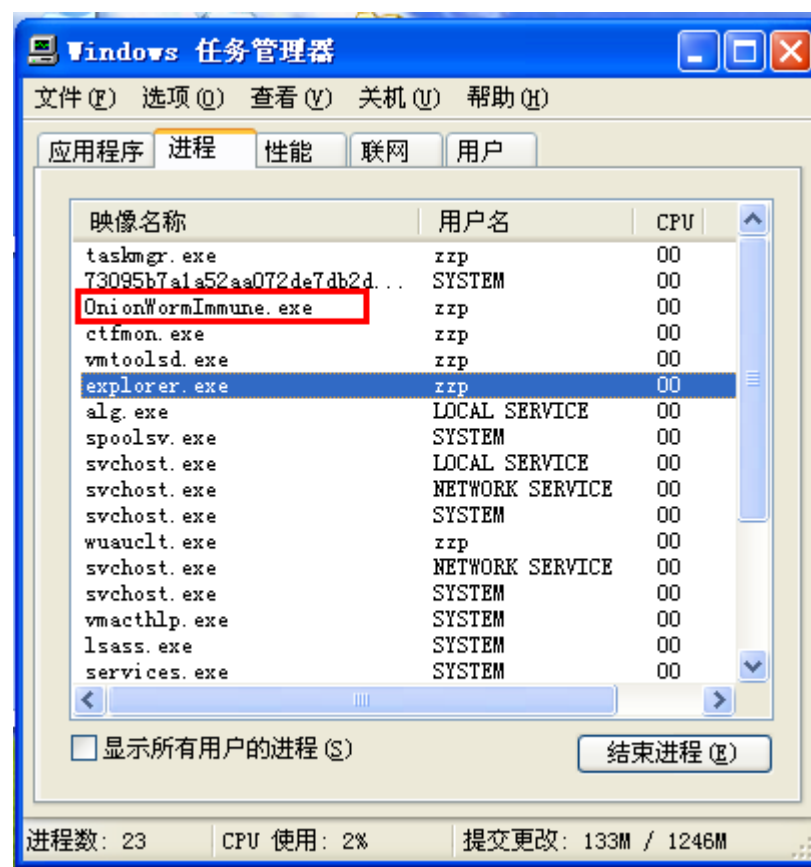
5. 在“组策略编辑器”上，右键“分配”，将规则启用。



四、终端层面

1. 免疫工具

由于批量终端的补丁安装需要一定时间，建议先用桌面管理类软件，在所有终端运行免疫工具（下载页面：<http://b.360.cn/other/onionwormimmune>），运行后可在任务管理器中检查其状态：



2. 关闭服务

如果免疫工具运行遇到问题，也可选择关闭 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

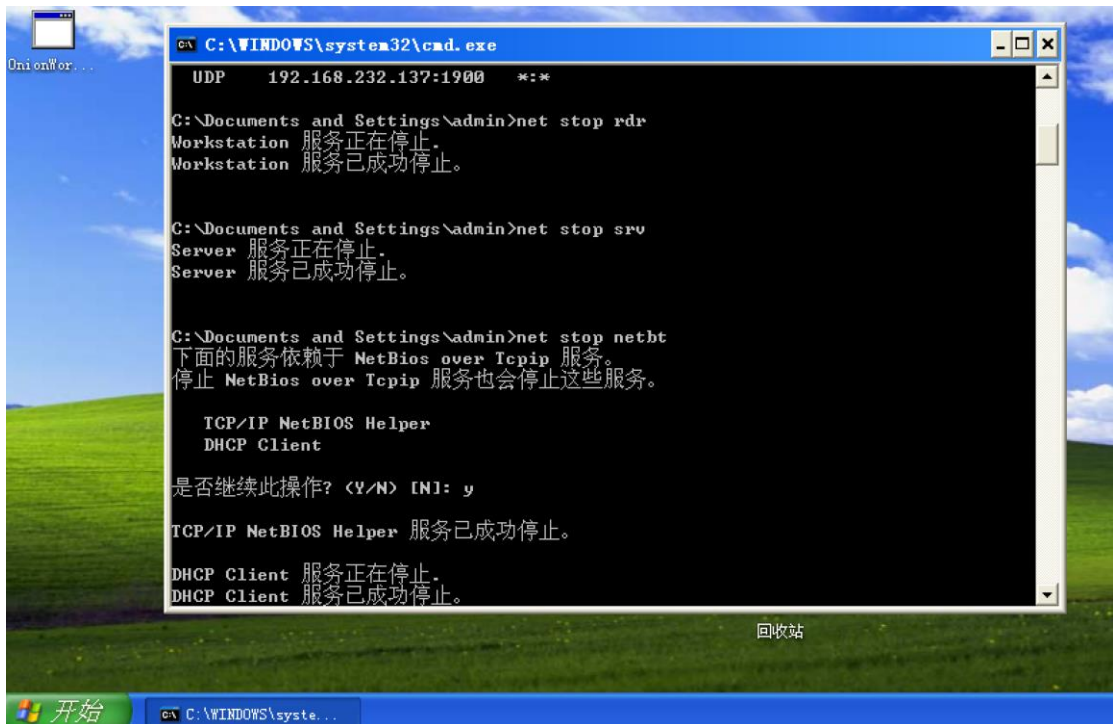
Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
TCP    127.0.0.1:1029          0.0.0.0:0               LISTENING
TCP    192.168.232.137:139    0.0.0.0:0               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.
```

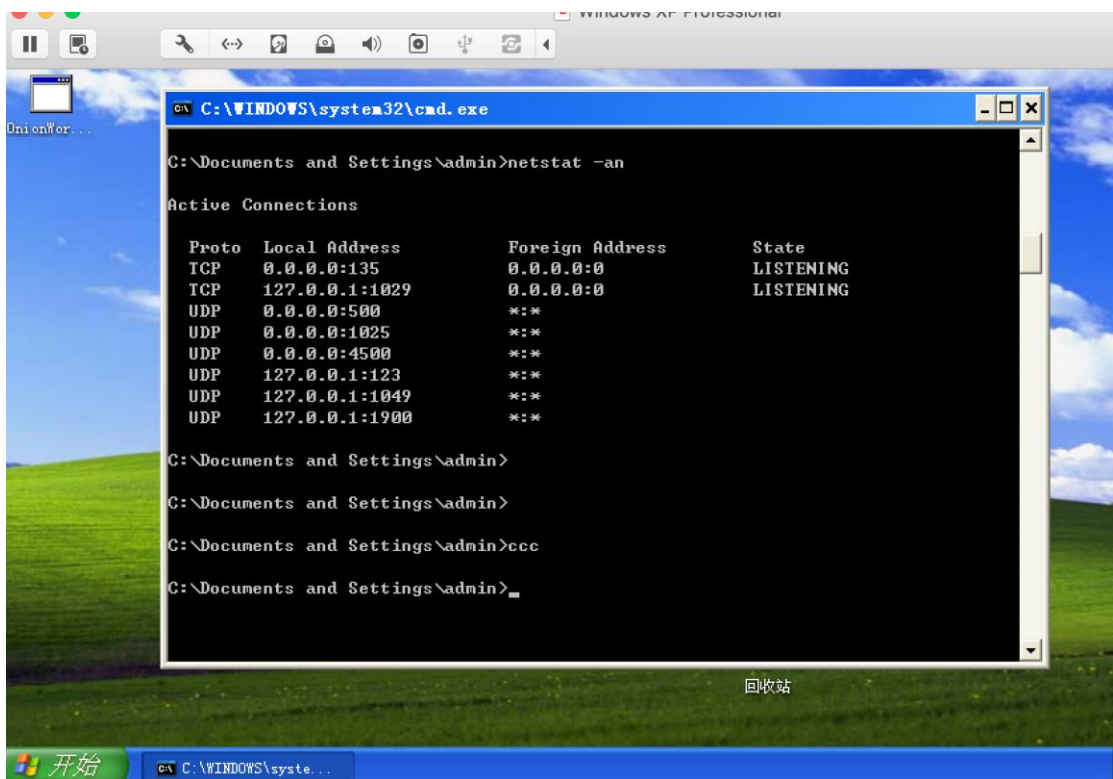
输入 net stop rdr 回车

net stop srv 回车

net stop netbt 回车



再次输入 netsta -an , 成功关闭 445 端口。也可用 “telnet 主机名 445” 的命令来验证终端端口已关闭。



3. 组策略调整

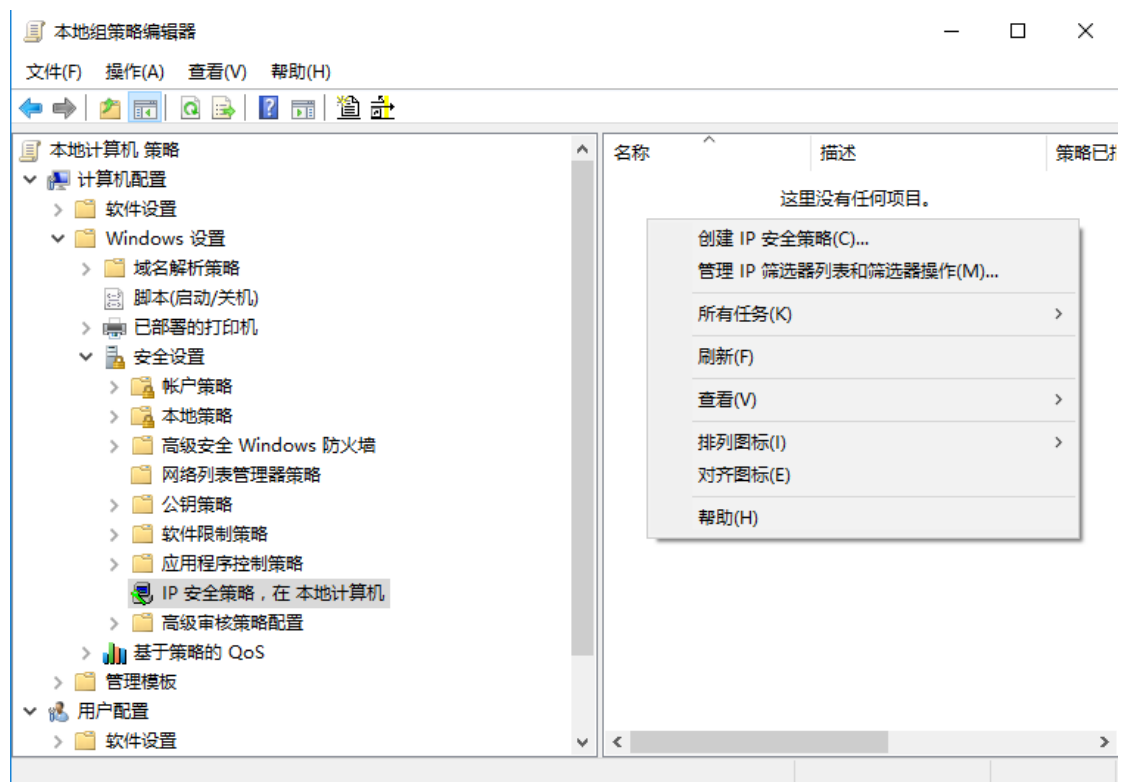
另一方式是用主机 ACL 策略封堵 445 端口。请注意，2、3、4 这三种方式，做到其中任意一个即可达到临时免疫的目的。

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”



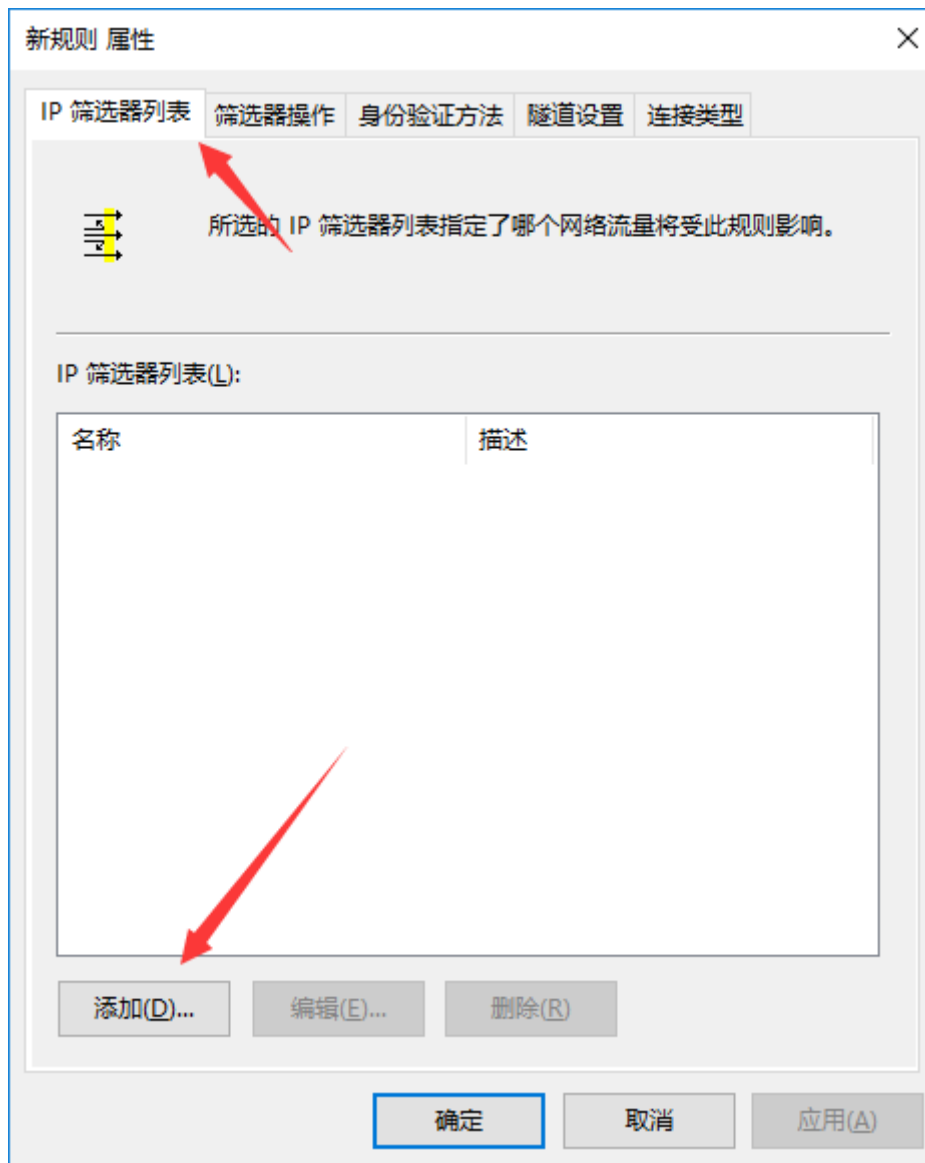
下一步->名称填写“封端口”，下一步->下一步->勾选编辑属性，并点完成



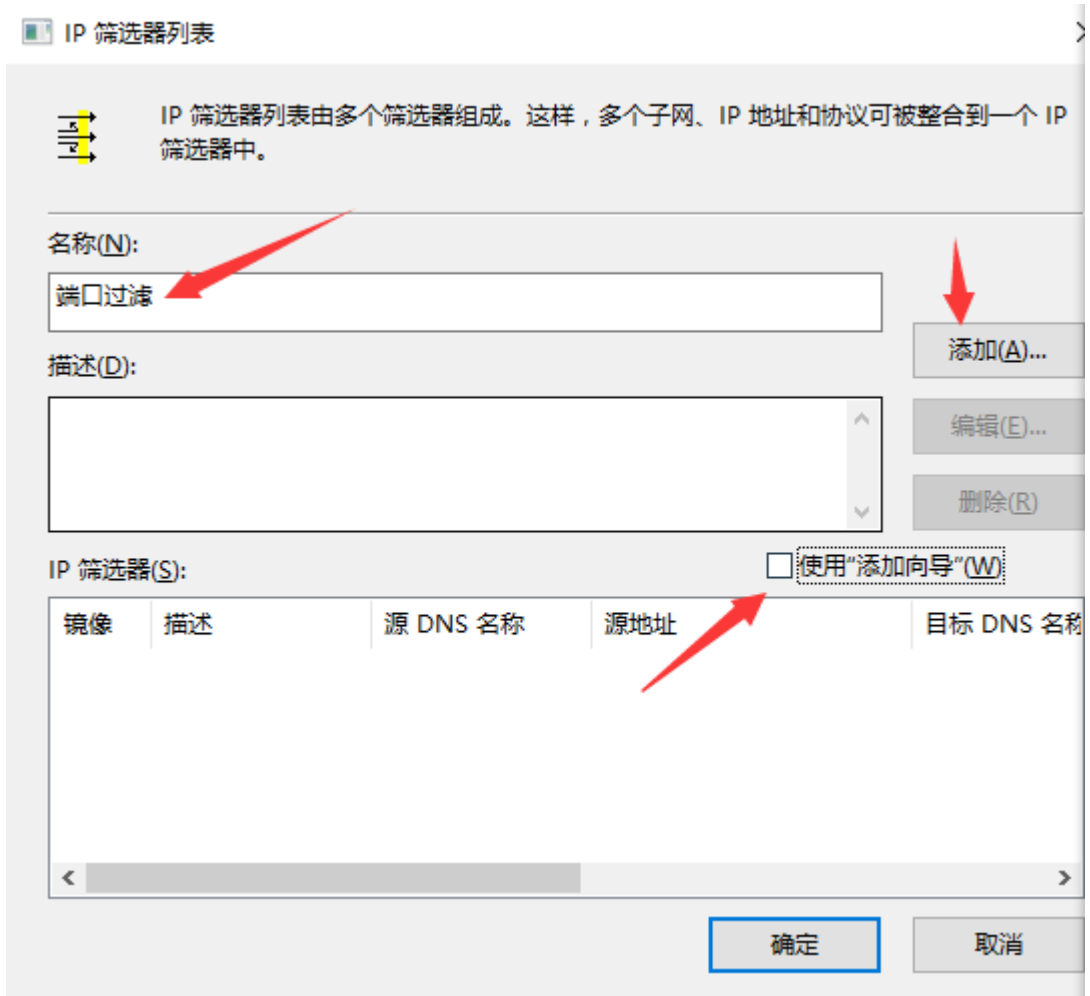
去掉“使用添加向导”的勾选后，点击“添加”



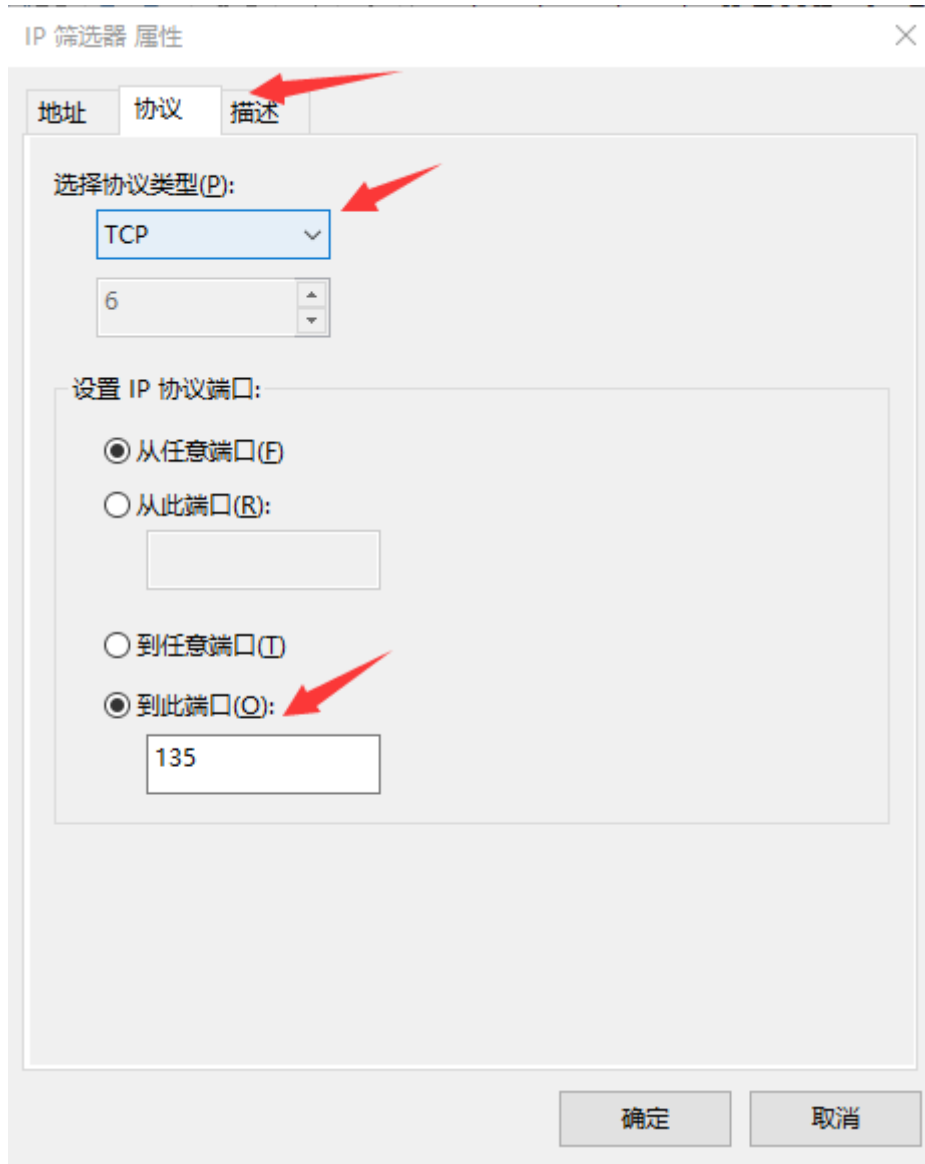
在新弹出的窗口，选择“IP 筛选列表”选项卡，点击“添加”



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”

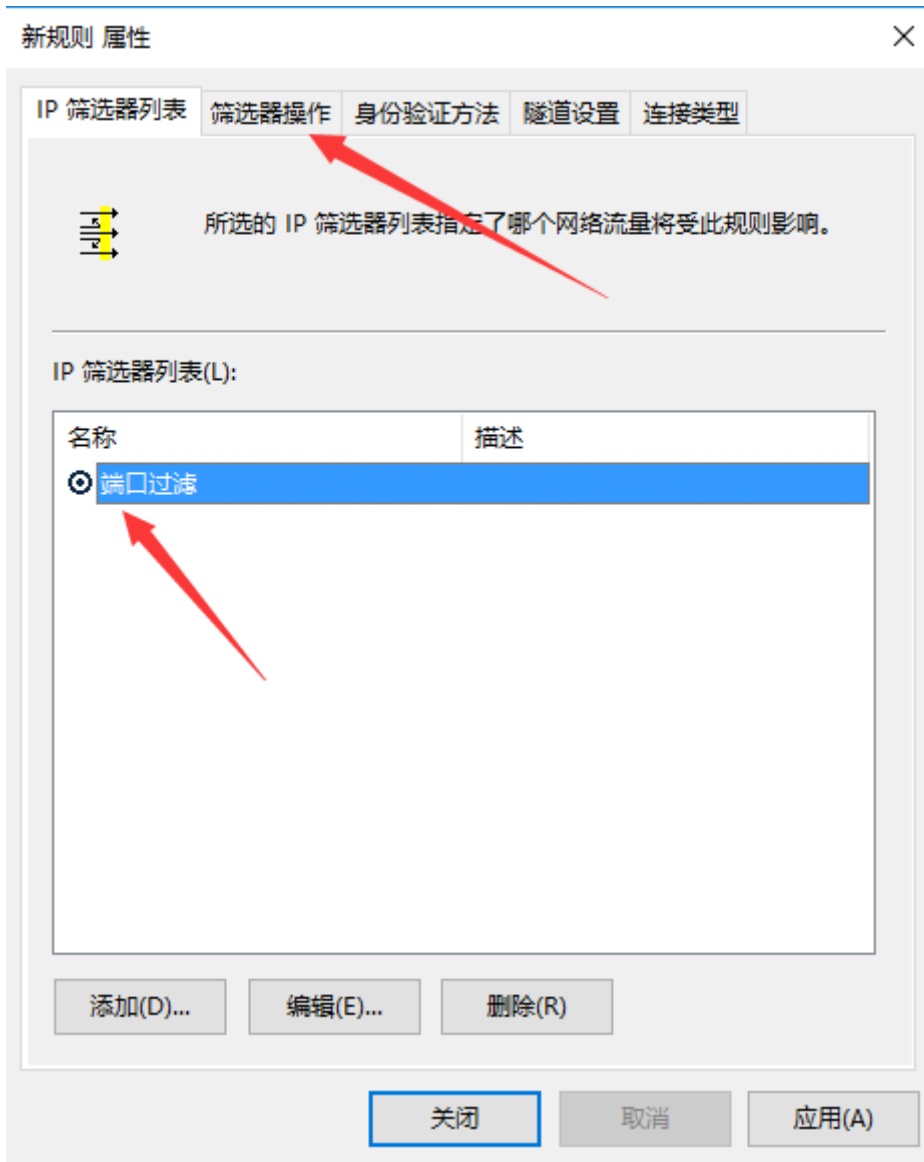


在新弹出的窗口中，“协议”选项卡下，选择协议和设置到达端口信息，并点确定。



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。

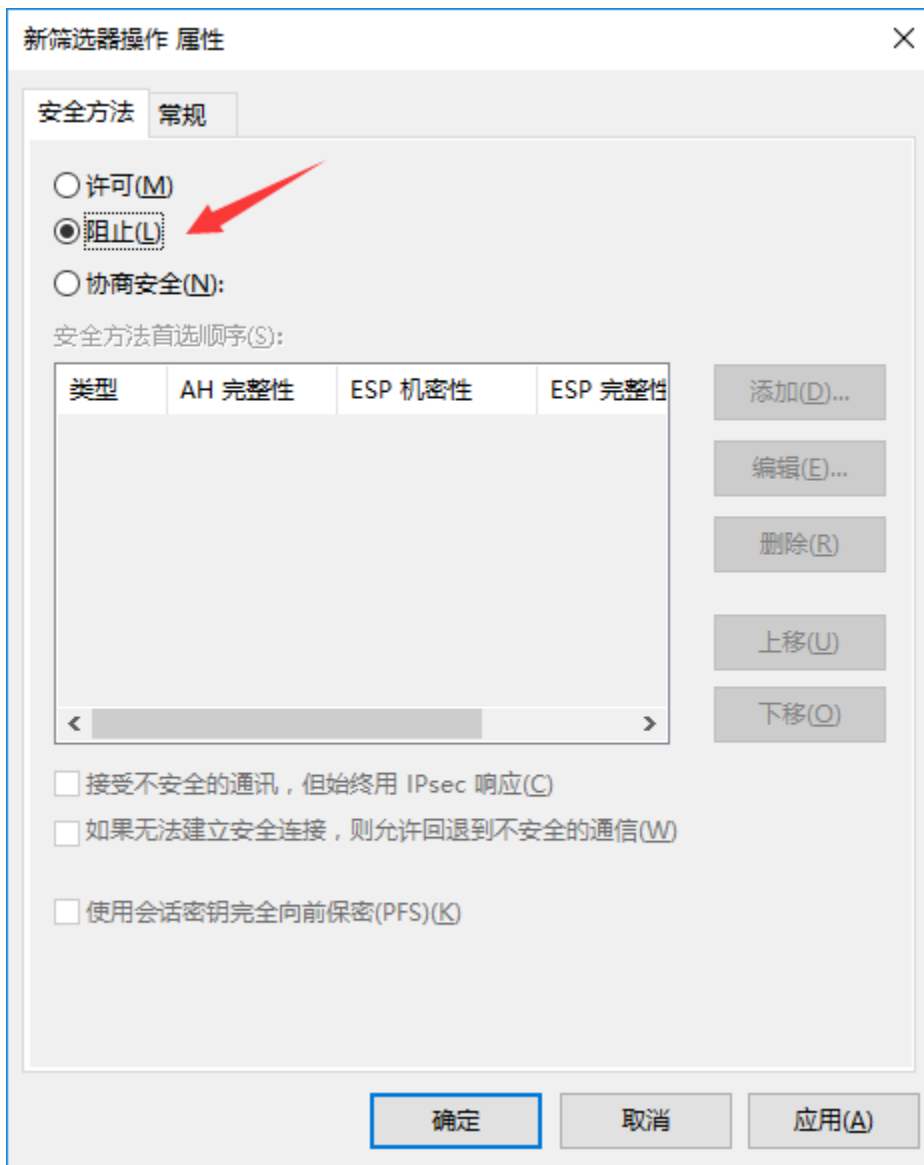
选中刚添加完成的“端口过滤”规则，然后选择“筛选器操作”选项卡。



去掉“使用添加向导”勾选，单击“添加”按钮



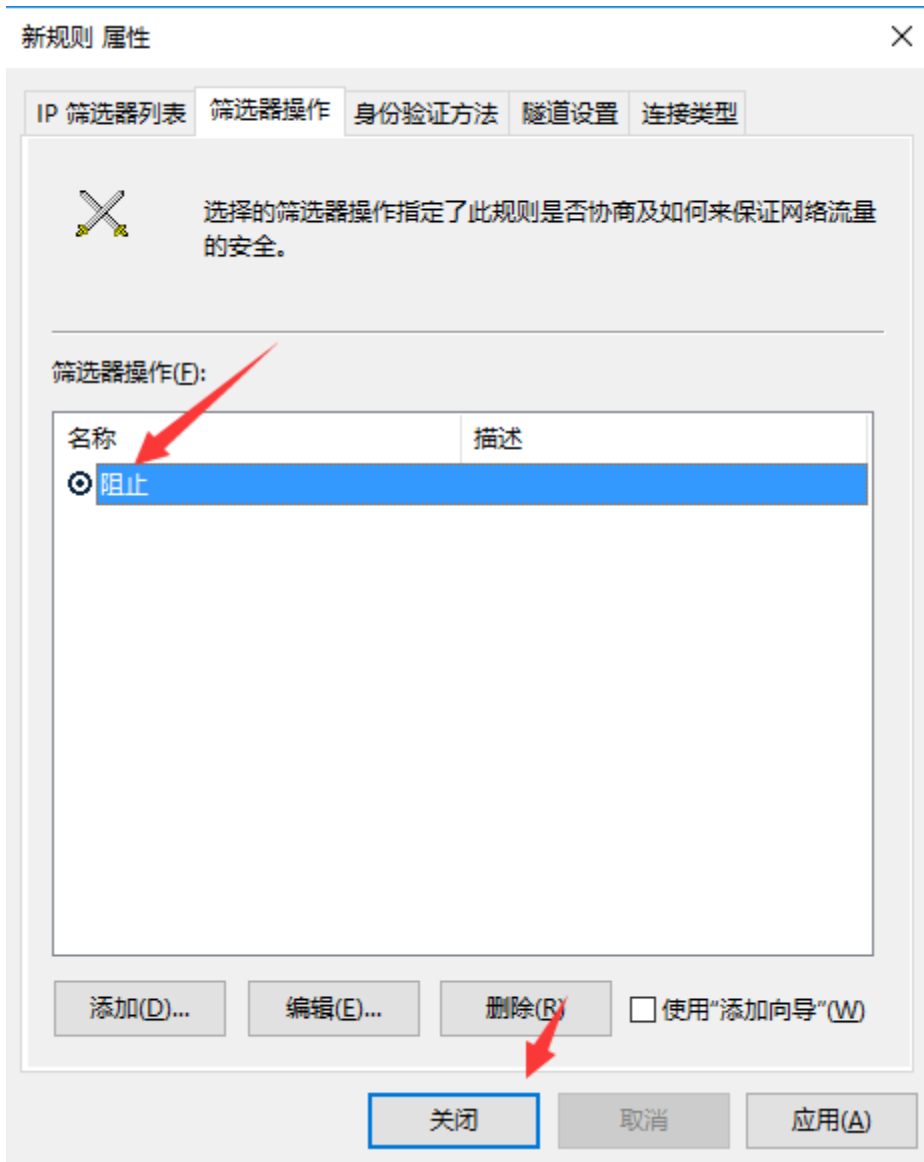
6. 选择“阻止”



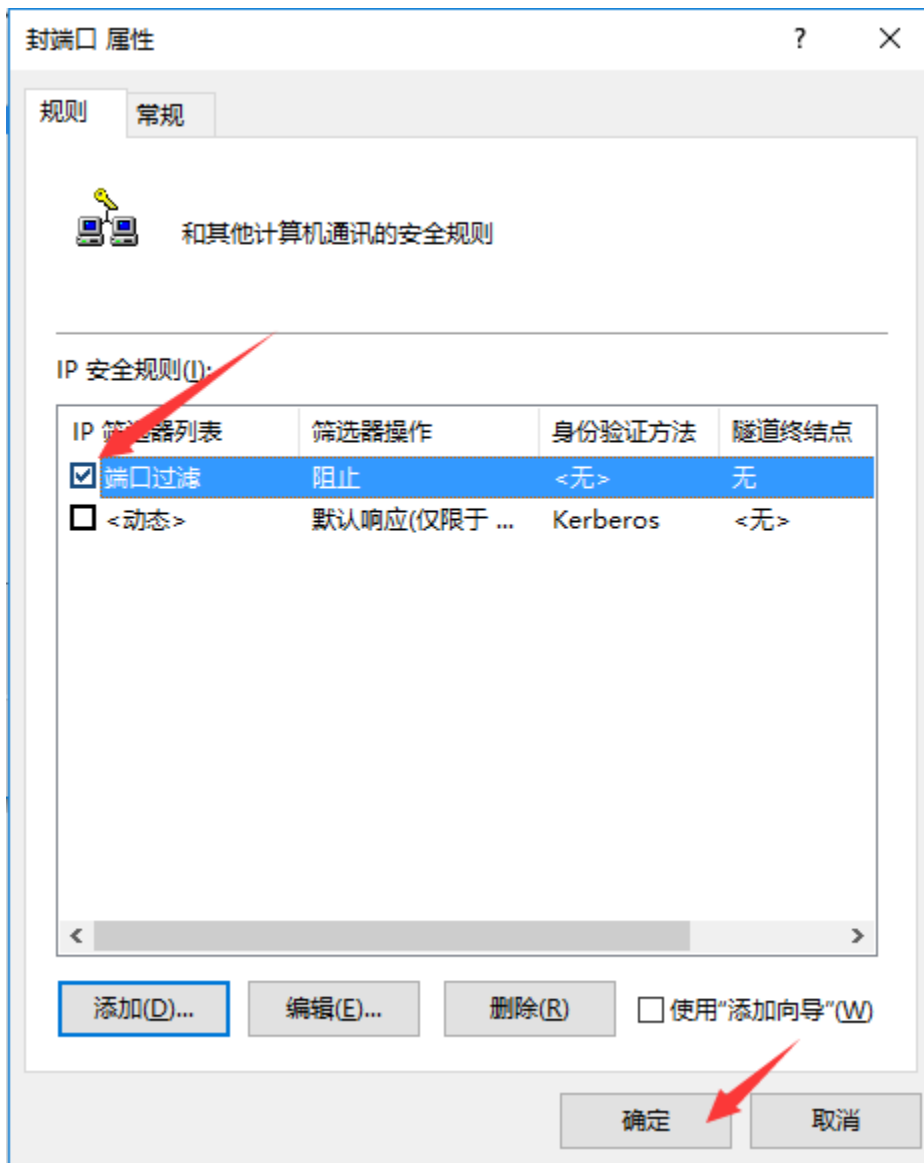
7. 选择“常规”选项卡，给这个筛选器起名“阻止”，然后“确定”。

点击

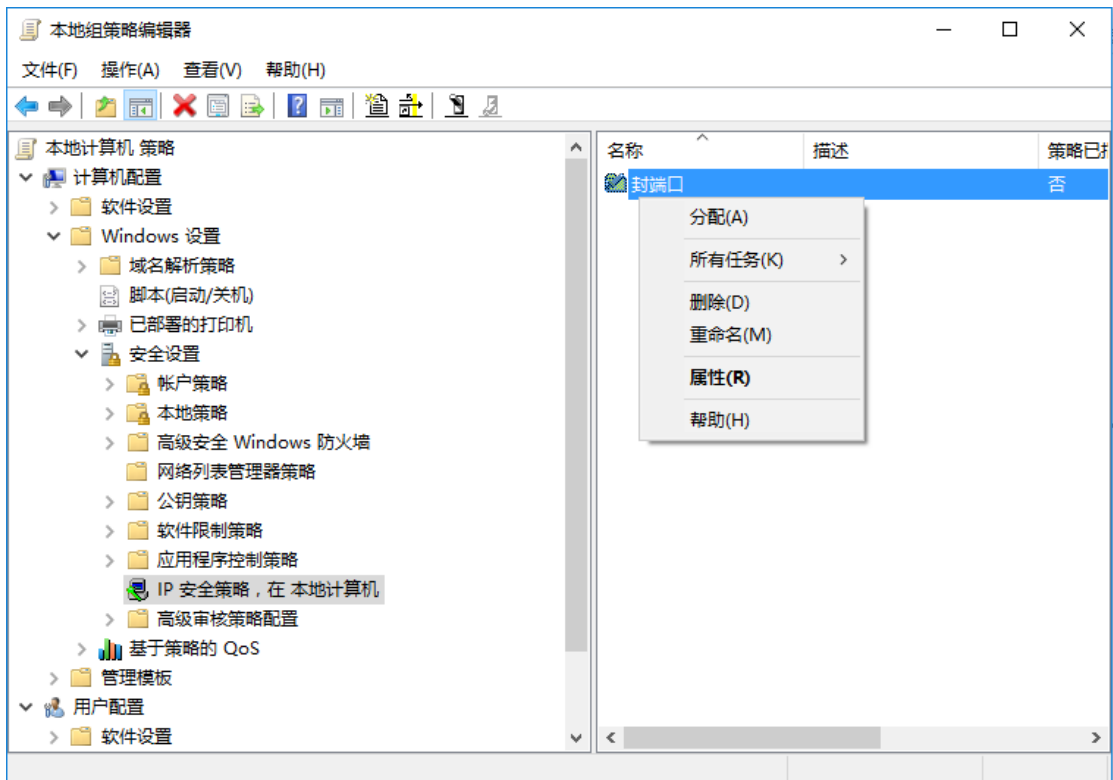
8. 确认“IP 筛选列表”选项卡下的“端口过滤”被选中。确认“筛选器操作”选项卡下的“阻止”被选中。然后点击“关闭”。



9. 确认安全规则配置正确。点击确定。



10. 在“组策略编辑器”上，右键“分配”，将规则启用。



4. 安装漏洞补丁

微软针对本次事件,对支持的操作系统在安全公告 MS17-010 中已发布相应补丁修复,对于部分已停服的 Win XP、2003 也已紧急发布补丁 KB4012598 修复。请在所有服务器及终端安装依据操作系统类型不同对应安装相应的补丁。下载来源:

MS17-010 Security Update:

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

KB4012598

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>

or 360 云盘:

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

根据不用的操作系统版本,手动安装以上补丁后,可直接修复此次“永恒之蓝”攻击的所利用的系统漏洞。

另外也可更新天擎控制中心补丁库升级到 1.0.1.2825 及以上版本,并安装其中包含的所有高危漏洞。

打补丁可能会对用户的现有业务系统、办公软件等造成影响,在生产服务器上安装前,需做好兼容性测试,避免影响业务。

五、周一开机及上线保障指南

打补丁是最终解决方案,免疫工具、关闭端口、停止服务是临时保证主机不感染的临时措施,只需做到一个即可达到效果。所以开机与上线的检查标准分 2 个等级:

- 补丁已安装

- 补丁未安装，临时措施已奏效

二者满足任意一条，该主机自身都不会感染，同时也不会感染其它主机，具备开机、上线的条件。只满足第二条的主机，需要后续跟进，直至完成补丁安装。

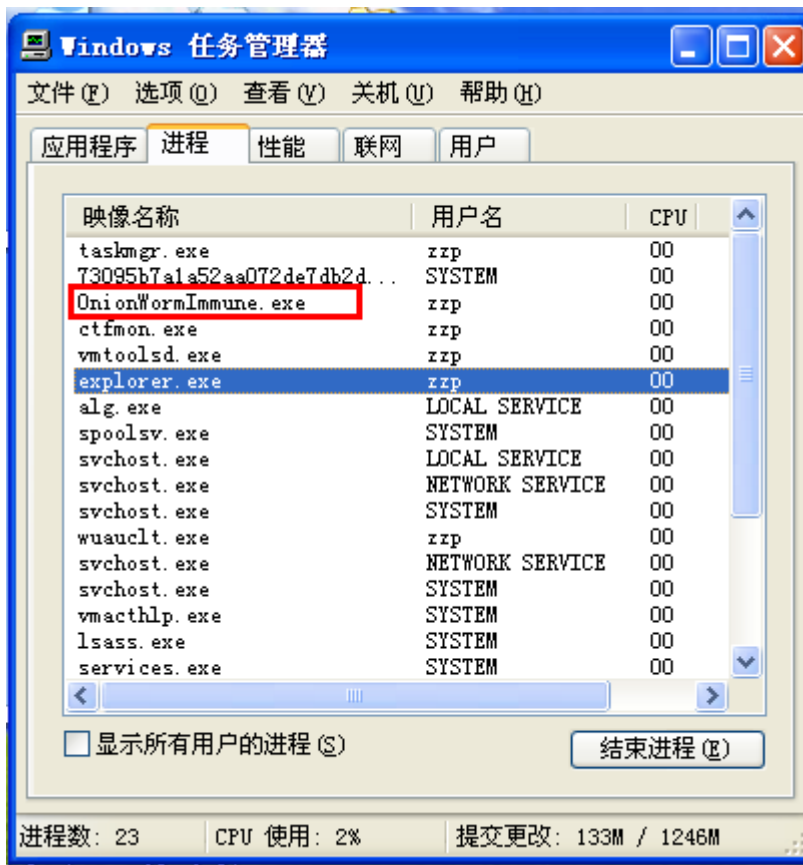
1. 补丁已安装检查方法：

从 Windows 控制面板中，检查已安装的补丁，确认相应补丁已安装

2. 临时措施生效检查方法：

满足以下任一条件即为合格：

A. 任务管理器检查免疫工具是否运行，可见 onionwormimmune.exe 进程。



B. 用同网段电脑运行以下命令，结果为“连接失败”即符合预期。

telnet <主机 IP> 445

第二部分——针对已使用 360 企业安全产品的运维人员

360 企业安全产品可增强企业内网对“永恒之蓝”的防御能力，提高 IT 安全运维的效率。天擎、天堤、天眼、虚拟化安全四类产品，均有针对性的操作建议。请参考以下各产品线的操作文档。



360企业安全产品应对永恒之蓝手册.rar

第三部分——未安装天擎的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 XP、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>



NSA武器库免疫工具

- 该漏洞危害可以远程攻破全球约70%Windows机器
- 该漏洞危害不需要用户任何操作，只要联网就可以远程攻击

 经检测，发现您的电脑存在该漏洞，请立即修复！

- EtemalBlue (永恒之蓝)
- EtemalChampion (永恒王者)
- EtemalRomance (永恒浪漫)
- EtemalSynergy (永恒协作)
- EmeraldThread (翡翠纤维)
- ErraticGopher (古怪地鼠)
- EskimoRoll (爱斯基摩卷)
- EducatedScholar (文雅学者)
- EclipsedWing (日食之翼)
- EsteemAudit(尊重审查)

立即修复

通过360安全卫士安装补丁