

# 针对“永恒之蓝”攻击紧急处置手册

## ( 蠕虫 WannaCry )



360安全监测与响应中心

2017年05月13日

## 目录

<b>第 1 章 隔离网主机应急处置操作指南.....</b>	<b>3</b>
首先确认主机是否被感染 .....	3
方式一：启用蠕虫快速免疫工具 .....	4
方式二：针对主机进行补丁升级 .....	4
方式三：关闭 445 端口相关服务 .....	5
方式四：配置主机级 ACL 策略封堵 445 端口 .....	6
<b>第 2 章 核心网络设备应急处置操作指南.....</b>	<b>19</b>
JUNIPER 设备的建议配置（示例）：.....	19
华三(H3C)设备的建议配置（示例）：.....	20
华为设备的建议配置（示例）：.....	21
Cisco 设备的建议配置（示例）：.....	21
锐捷设备的建议配置（示例）：.....	22
<b>第 3 章 互联网主机应急处置操作指南.....</b>	<b>22</b>

# 第1章 隔离网主机应急处置操作指南

## 首先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）。若客户存在该主机备份，则启动备份恢复程序。

### 如果主机未被感染：

则存在四种方式进行防护，均可以避免主机被感染。针对未感染主机，方式二是属于彻底根除的手段，但耗时较长；其他方式均属于抑制手段，其中方式一效率最高。

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。

## 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。



## 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：

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

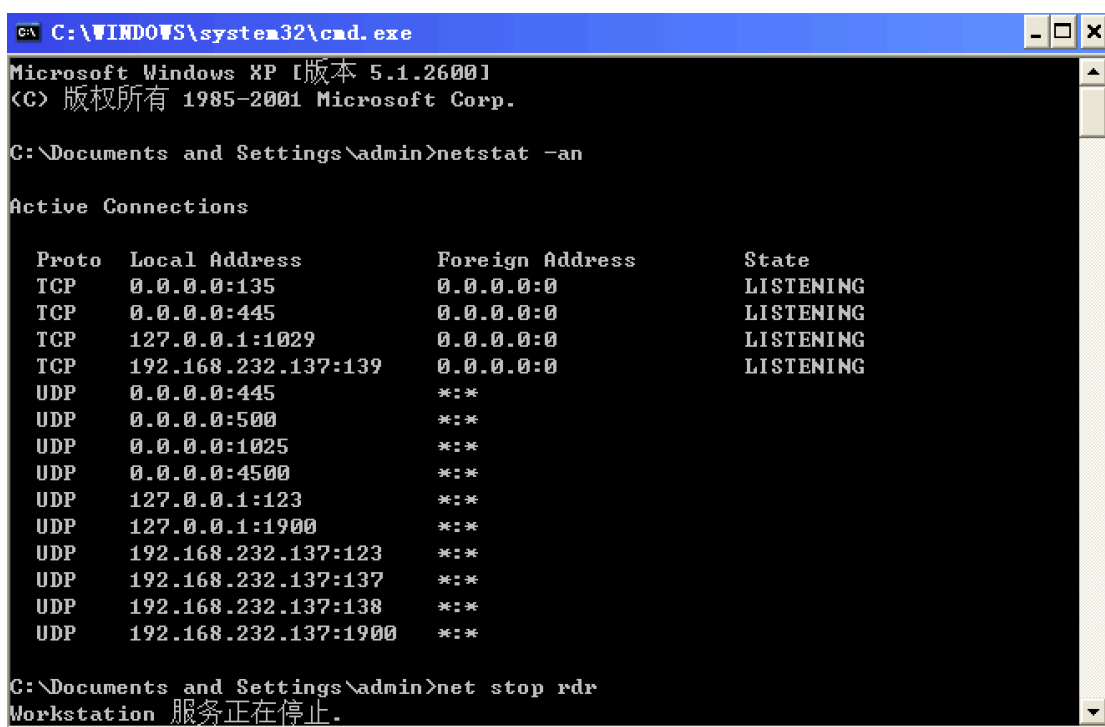
快速下载地址:

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

## 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

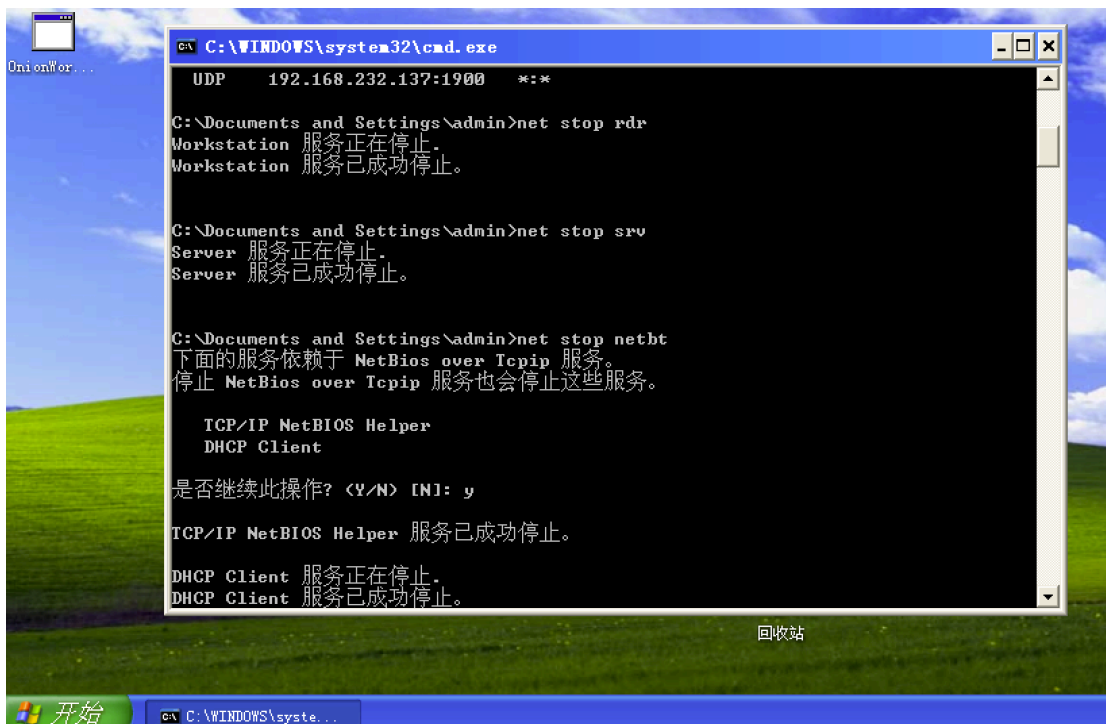
Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              0.0.0.0:0              LISTENING
TCP    0.0.0.0:445              0.0.0.0:0              LISTENING
TCP    127.0.0.1:1029           0.0.0.0:0              LISTENING
TCP    192.168.232.137:139     0.0.0.0:0     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

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

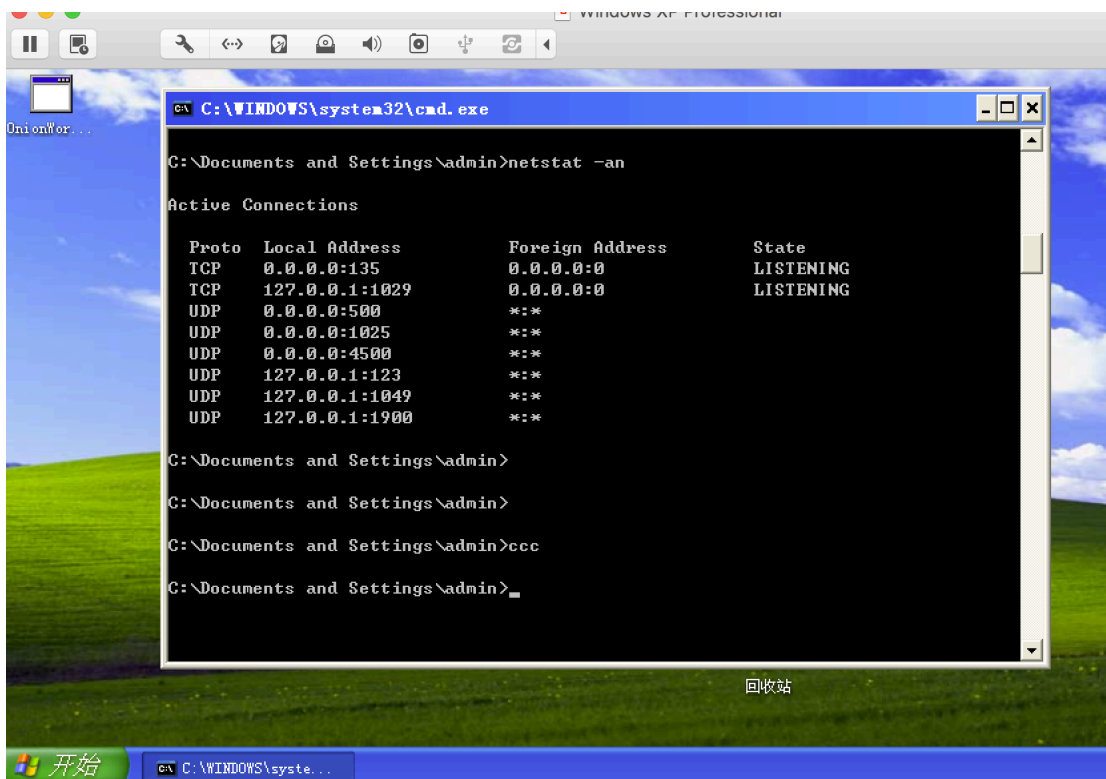
输入 net stop rdr 回车

net stop srv 回车

net stop netbt 回车



再次输入 netsta -an，成功关闭 445 端口。

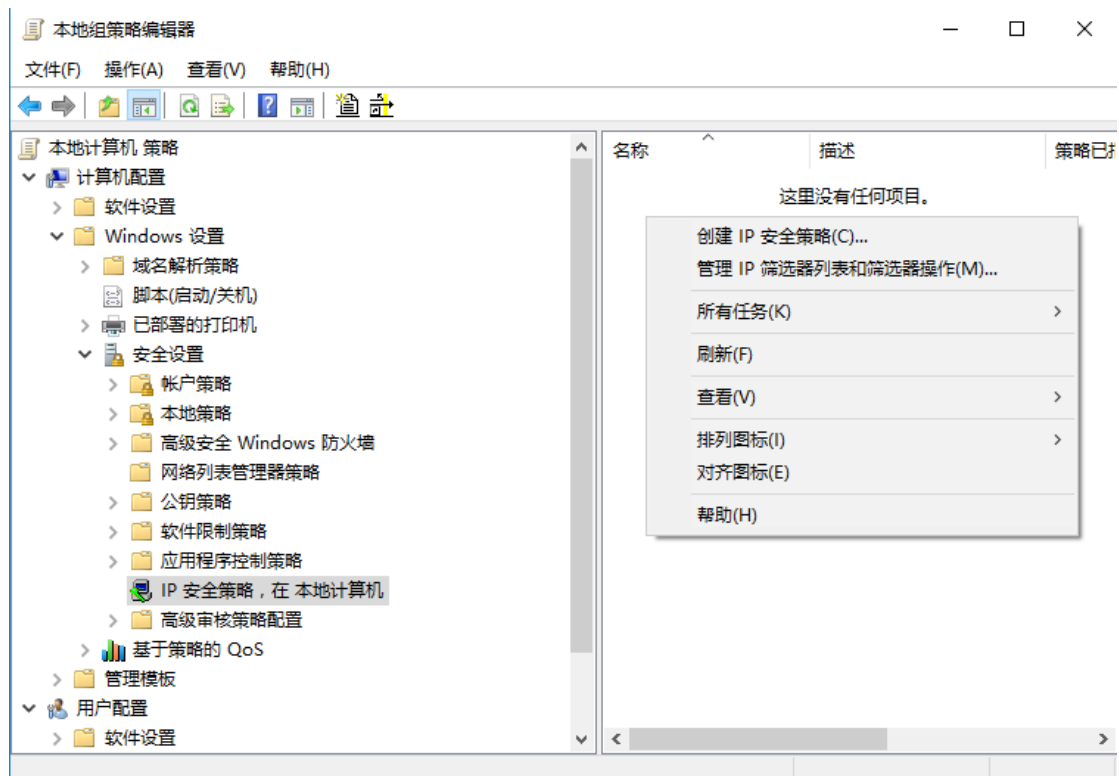


## 方式四：配置主机级 ACL 策略封堵 445 端口

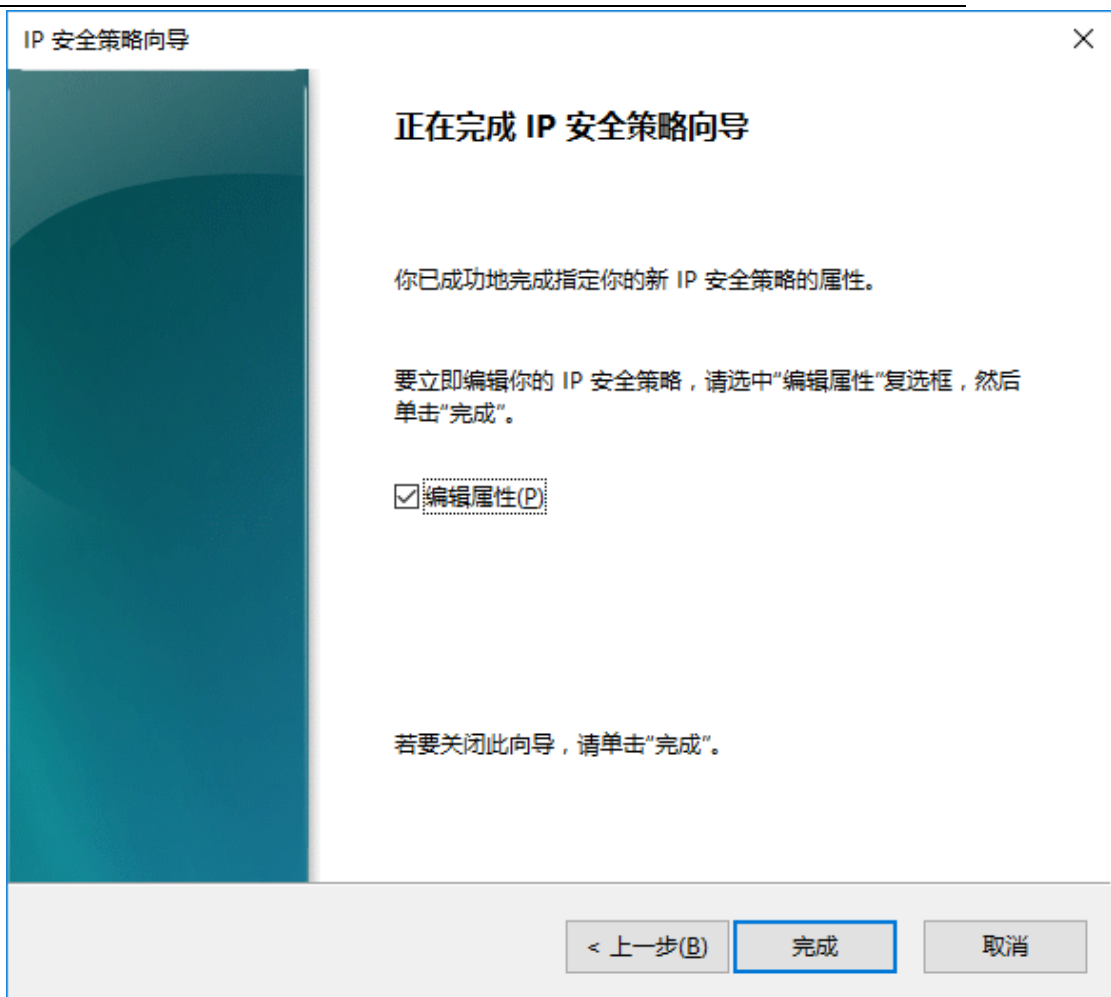
通过组策略 IP 安全策略限制 Windows 网络共享协议相关端口

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”

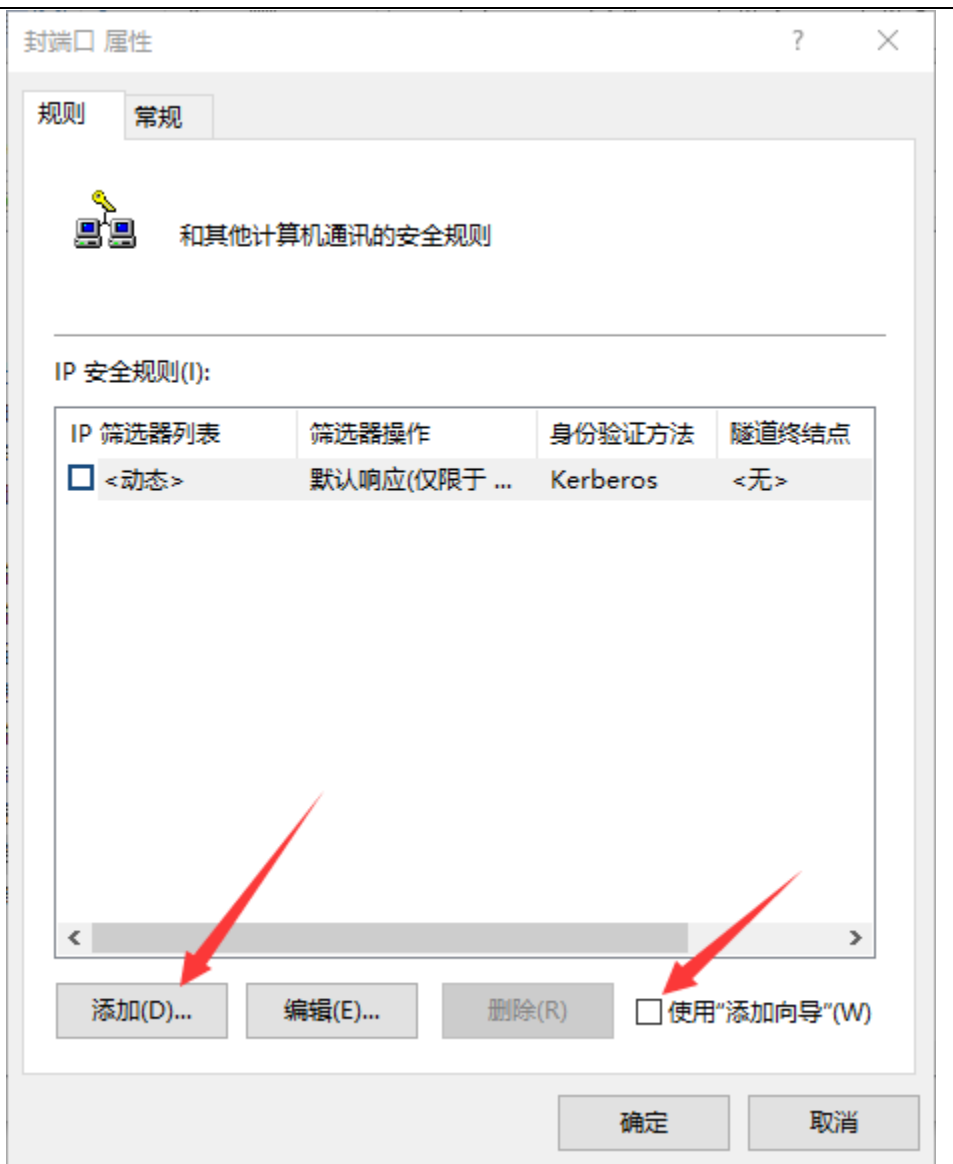


下一步->名称填写“封端口”，下一步->下一步->勾选编辑属性，并点完成

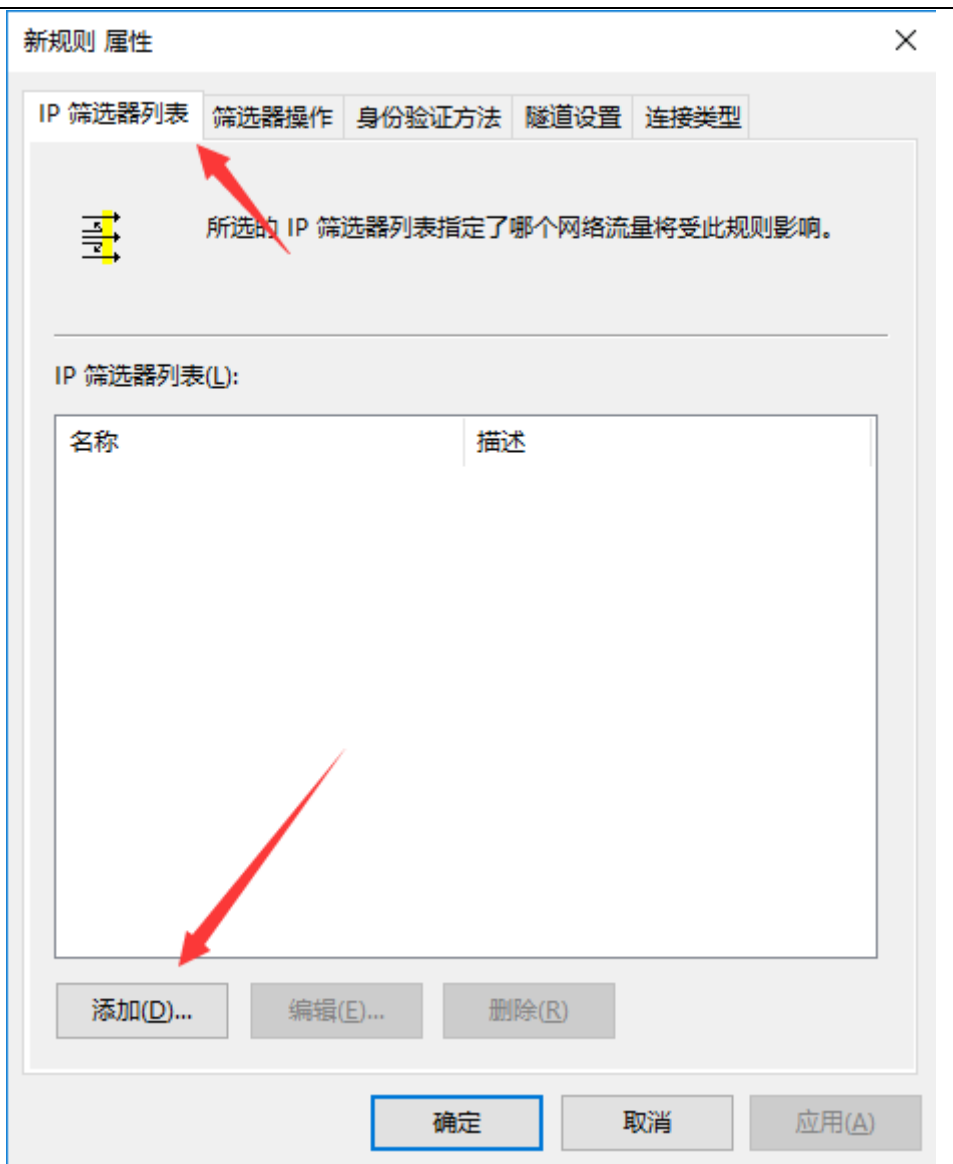


去掉“使用添加向导”的勾选后，点击“添加”

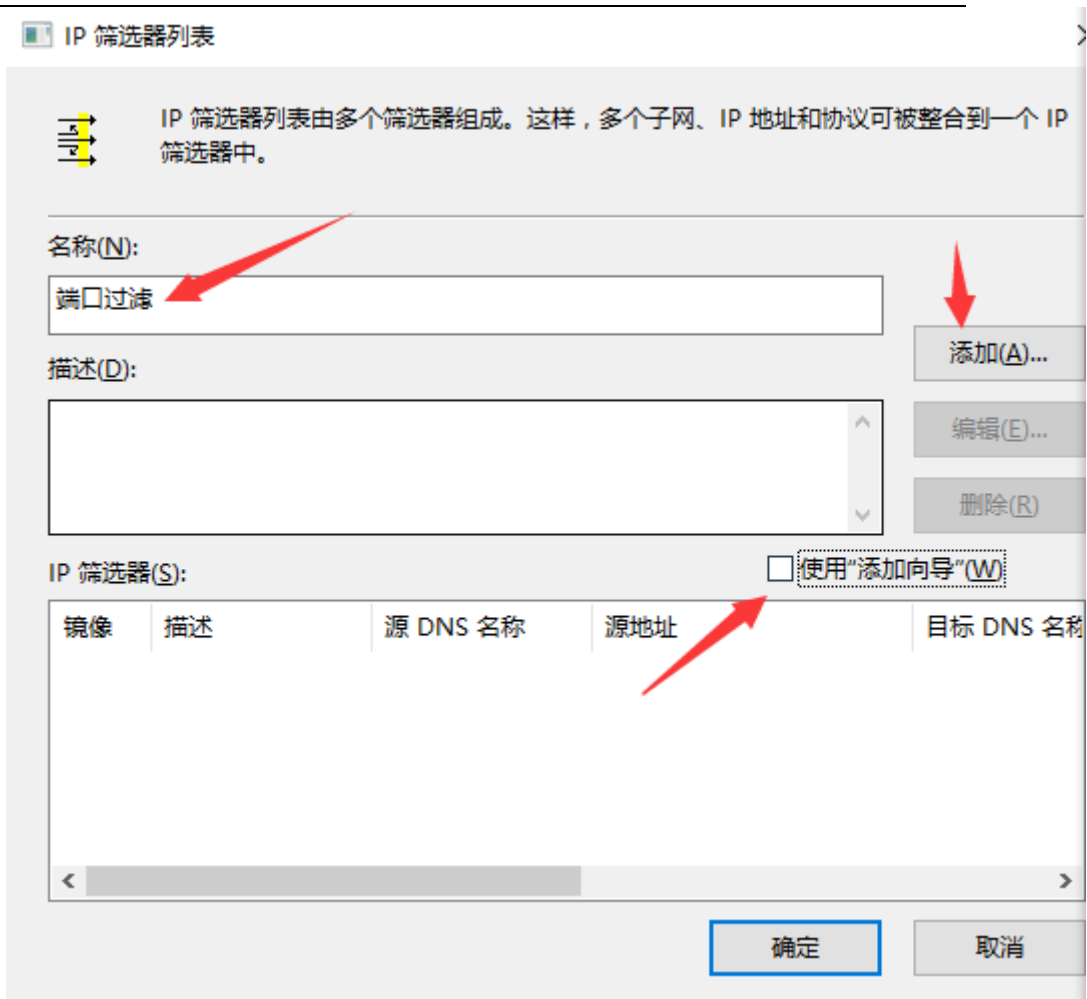




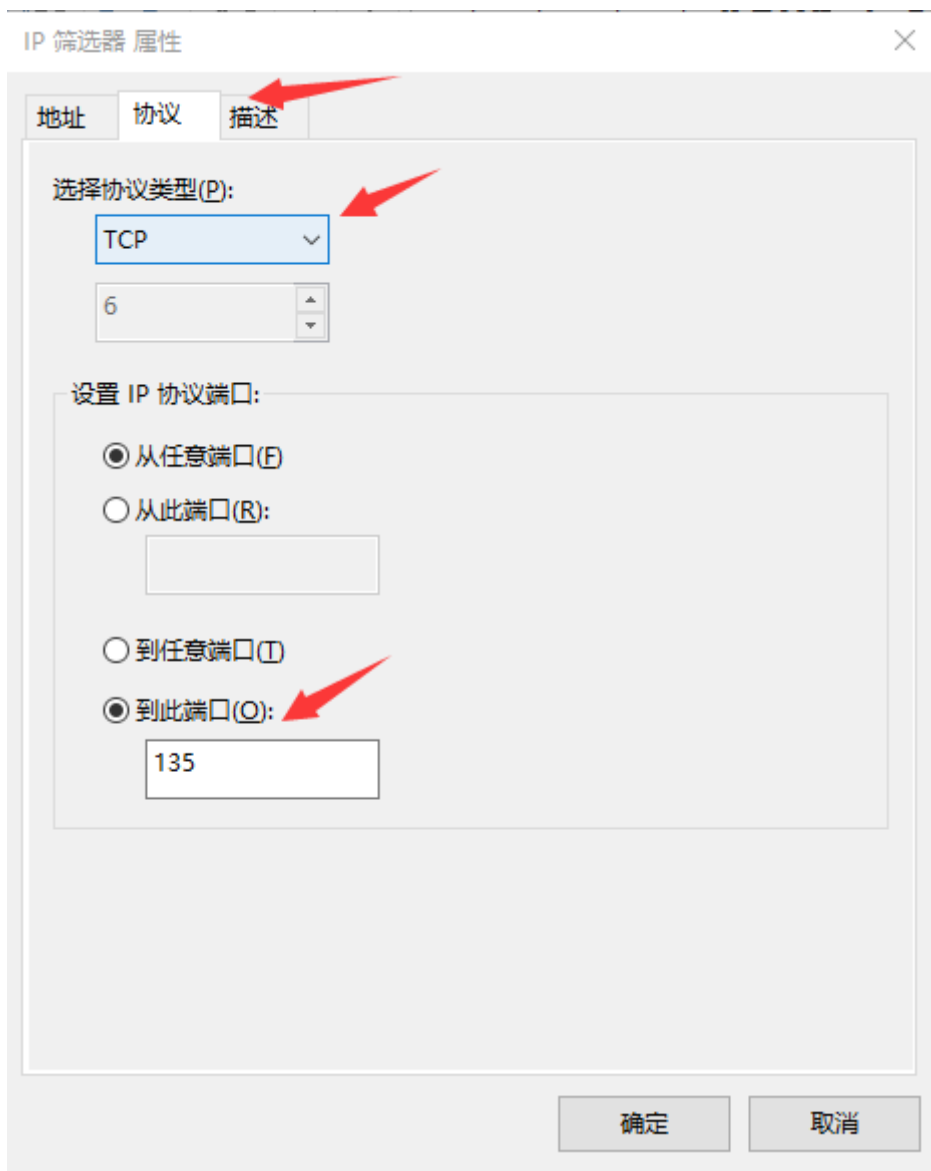
在新弹出的窗口，选择“IP 筛选列表”选项卡，点击“添加”



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”

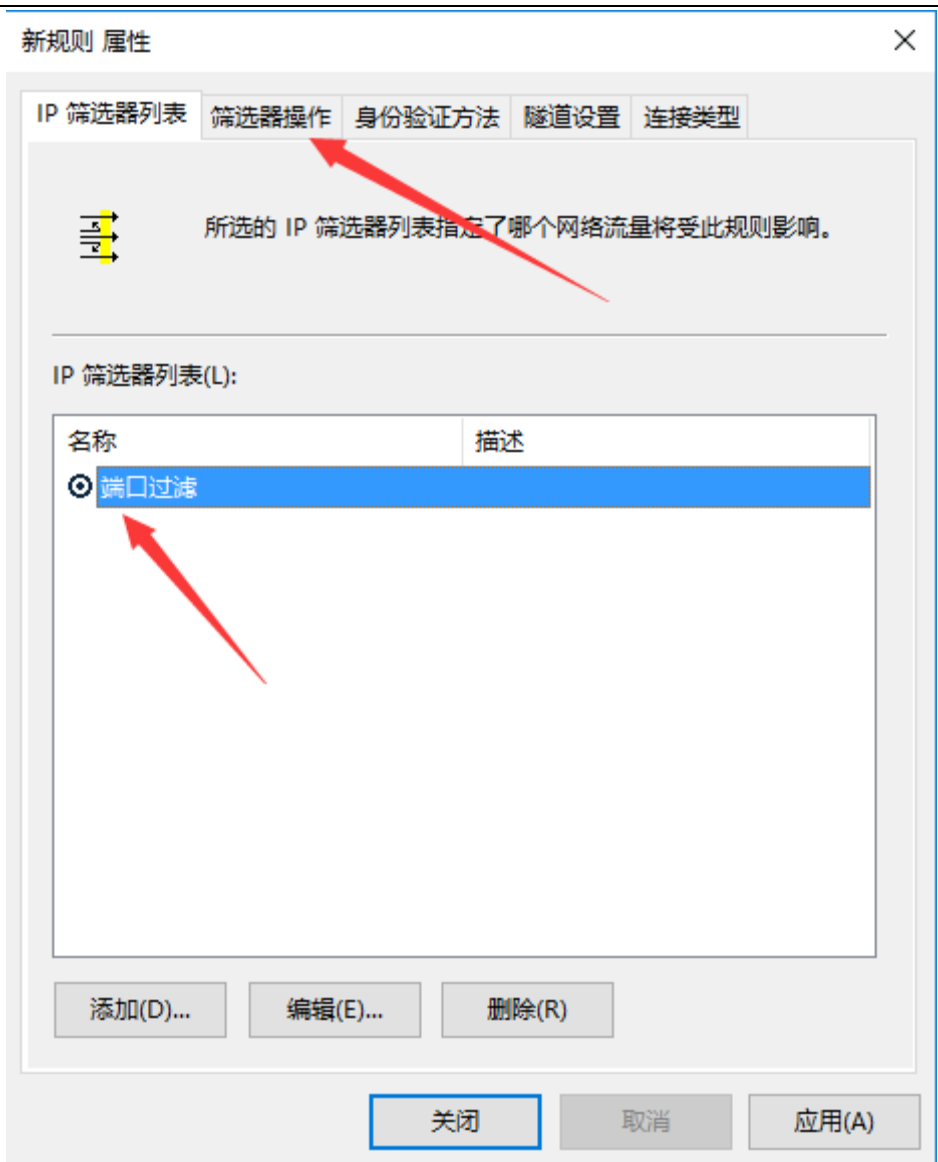


在新弹出的窗口中，“协议”选项卡下，选择协议和设置到达端口信息，并点确定。



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。



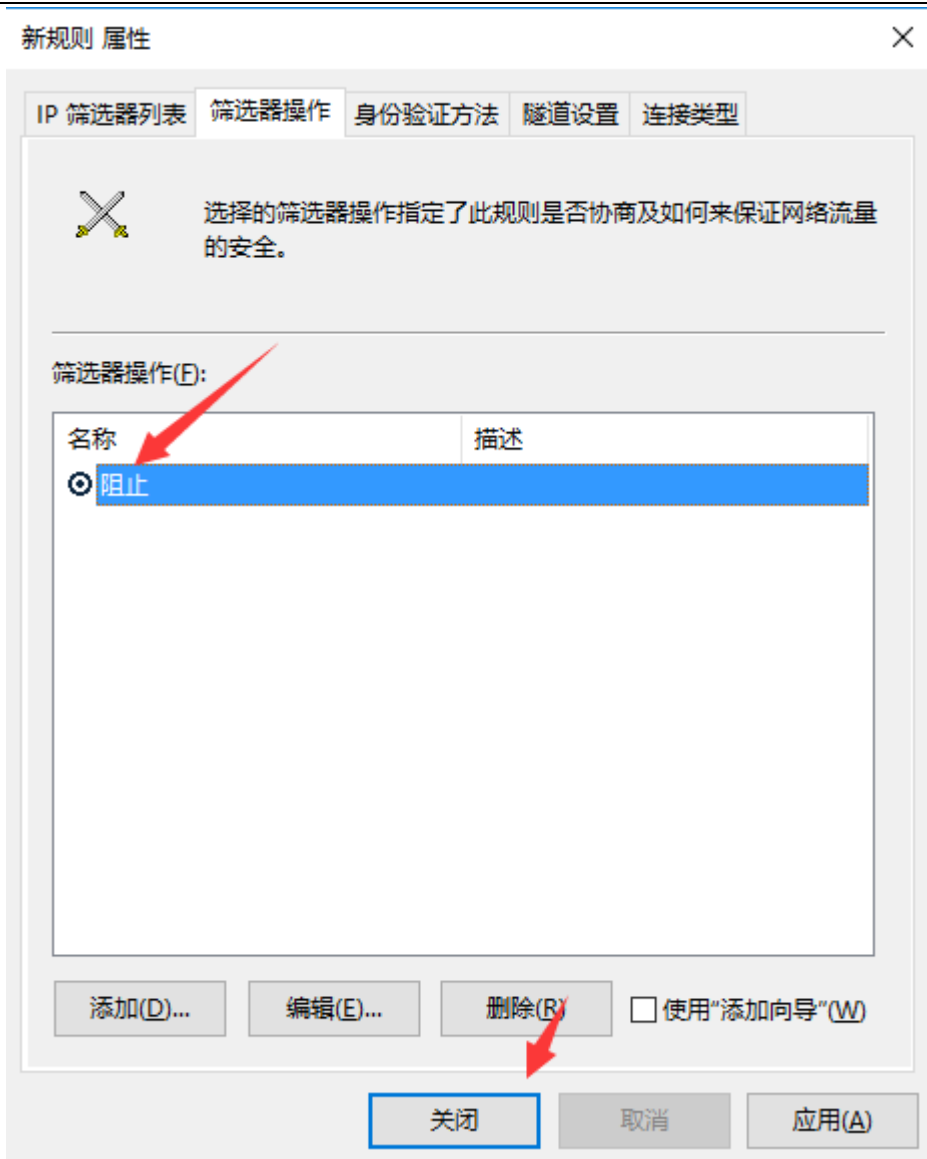
去掉“使用添加向导”勾选，单击“添加”按钮



1. 选择“阻止”

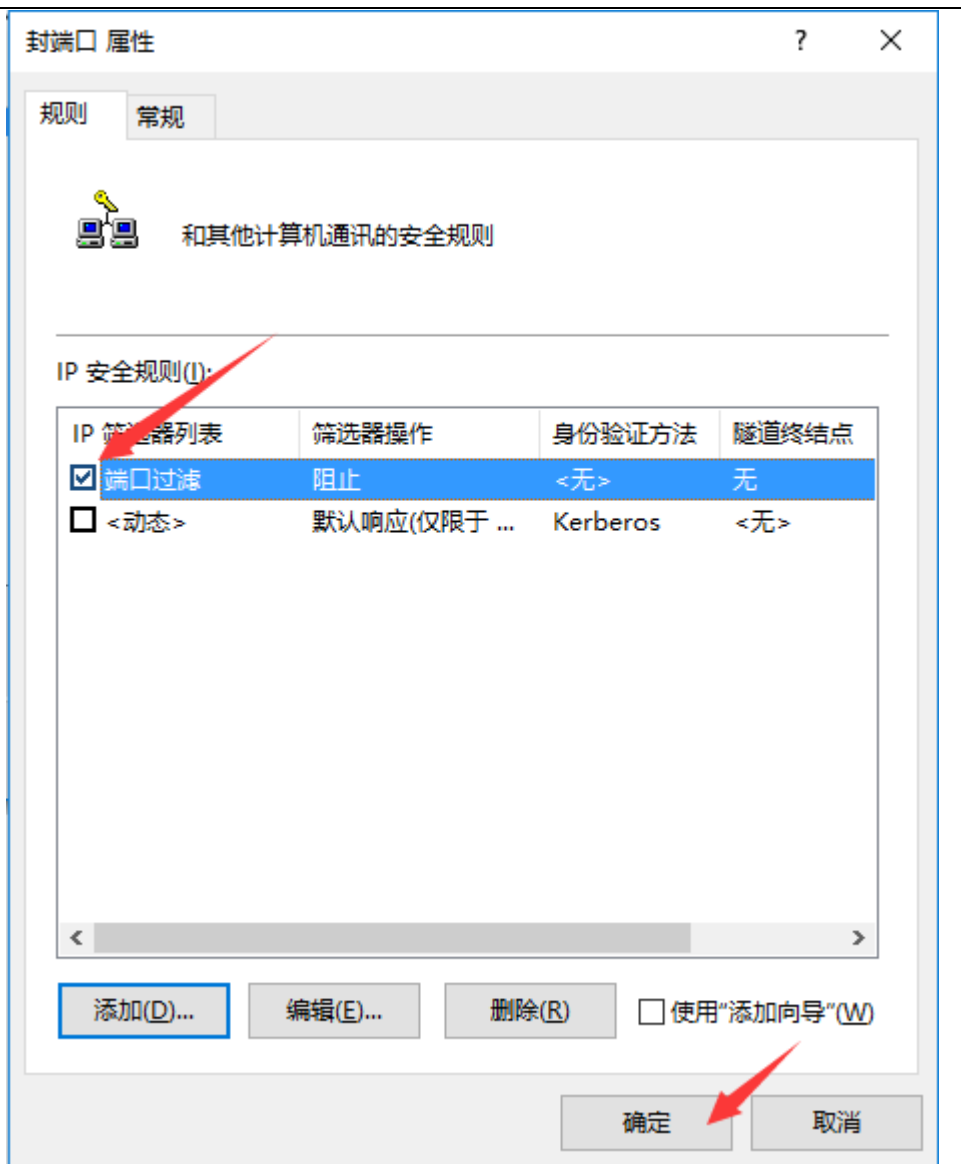


2. 选择“常规”选项卡，给这个筛选器起名“阻止”，然后“确定”。  
点击
3. 确认“IP 筛选列表”选项卡下的“端口过滤”被选中。确认“筛选器操作”选项卡下的“阻止”被选中。然后点击“关闭”。

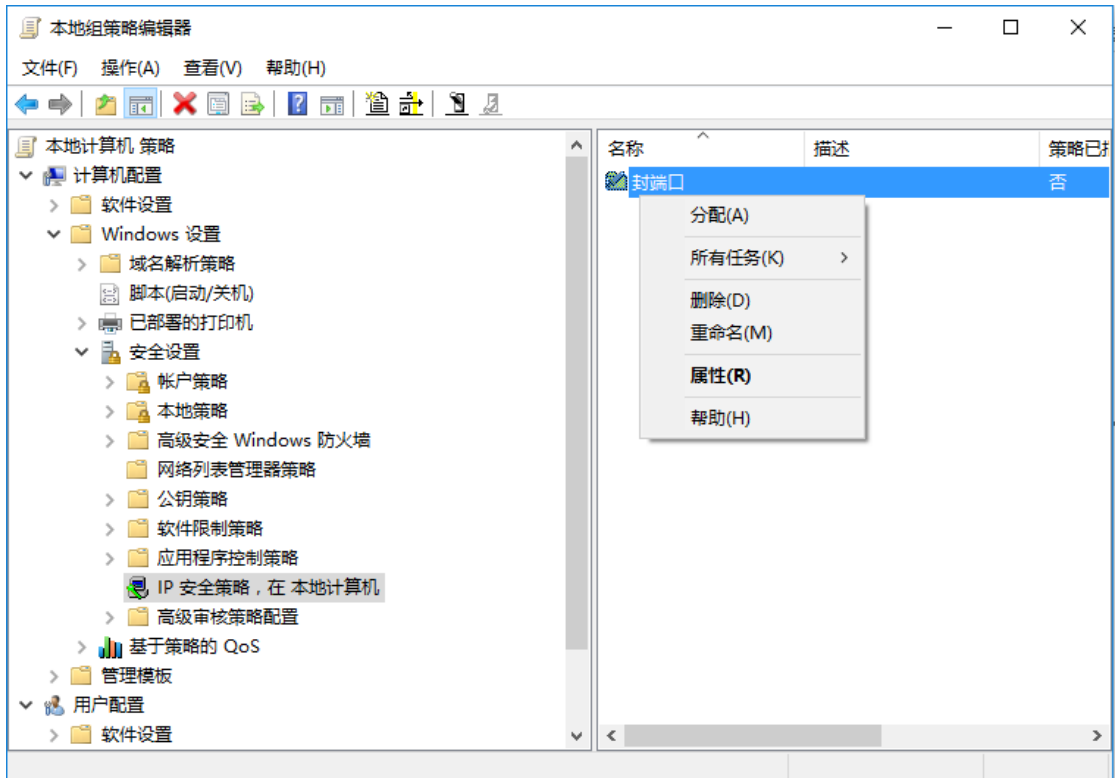


4. 确认安全规则配置正确。点击确定。





5. 在“组策略编辑器”上，右键“分配”，将规则启用。



## 第2章 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 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。

### 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
```

---

## 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
```

### 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
```

### 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

### 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

## 第3章 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！

- EternalBlue (永恒之蓝)
- EternalChampion (永恒王者)
- EternalRomance (永恒浪漫)
- EternalSynergy (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