

# 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

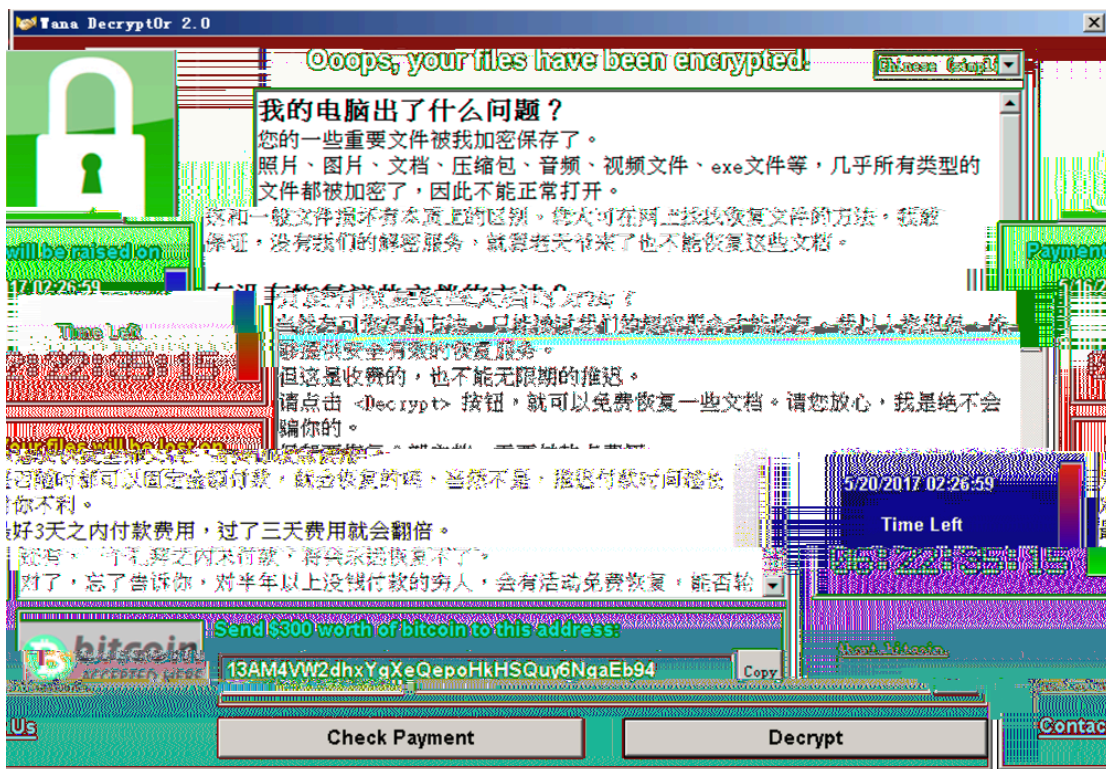
2017年05月13日

<b>第 1 章 隔离网主机应急处置操作指南.....</b>	<b>3</b>
先    主    .....	3
一：    免    具.....	4
二：    主    丁升.....	4
三：关    445    关    务.....	5
：    主    ACL        445    .....	6
<b>第 2 章 核心网络设备应急处置操作指南.....</b>	<b>19</b>
JUNIPER        （    例）：.....	19
华三(H3C)        （    例）：.....	20
华为            （    例）：.....	21
CISCO            （    例）：.....	21
（    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 主 作 南

先 主

会 下 付 :



主 :

则 主 ( )。 主 份, 则 动 份

主 :

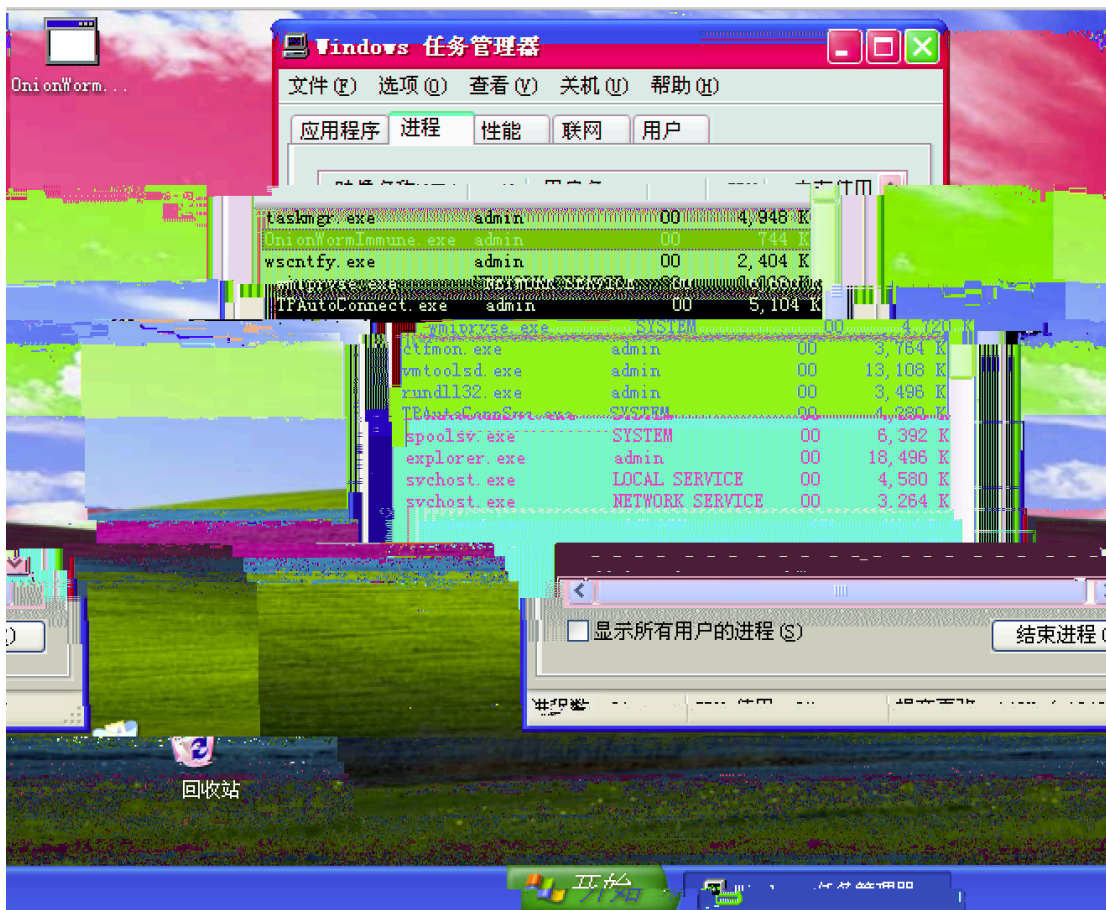
则 , 以 免主 。 主 , 二 于 , 但 ; 其他 于 制 , 其中 一

从 上, 360 先 一 制, 再 二

## 一： 免 具

免 具 下 址：<http://dl.b.360.cn/tools/OnionWormImmune.exe>

击 运行 OnionWormImmune.exe 免 具， 任务 管理器 中 。



## 二： 主 丁升

具包 关 于 MS17-010 丁升，  
winxp\_sp3 win10、win2003 win2016 全 列 丁。

下 址：

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

下 :

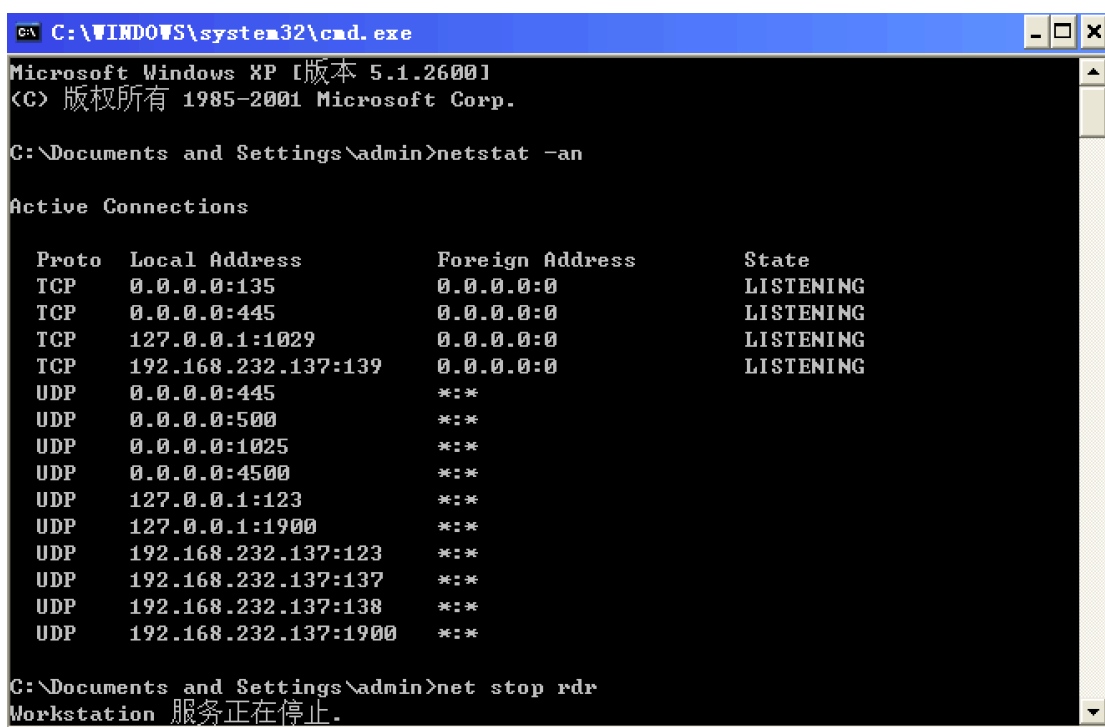
<https://yunpan.cn/cXLwmvHrMF3WI>

614d

### 三：关 445 关 务

击 单, , cmd, 。

入 令 netstat -an



```
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

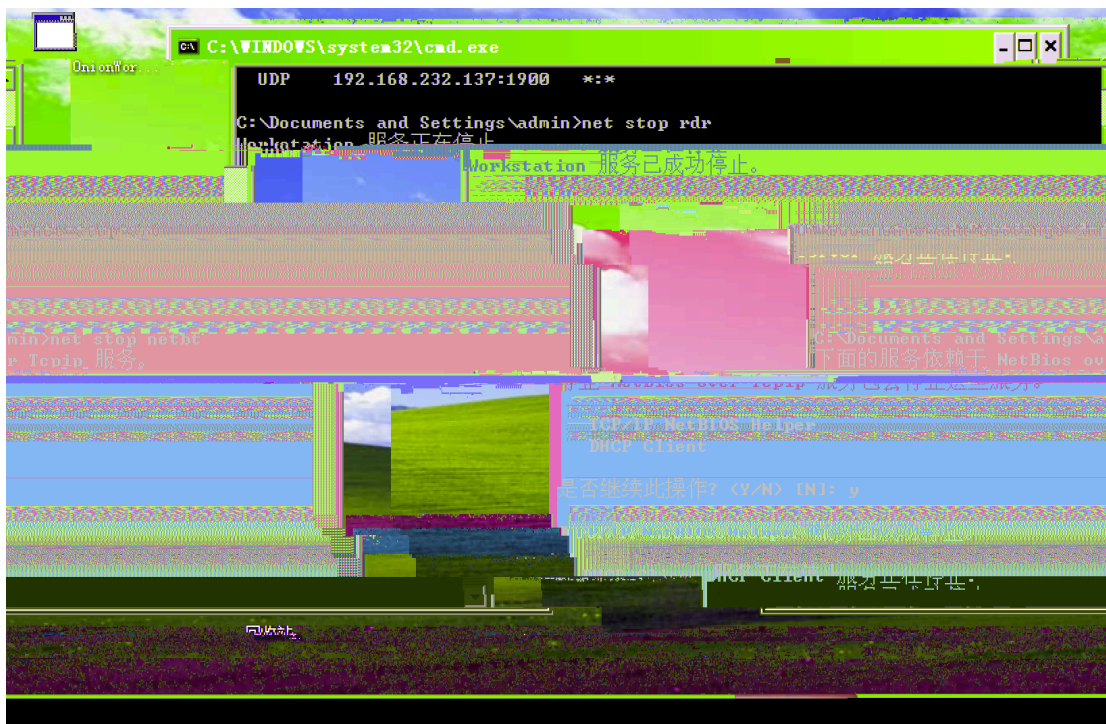
Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              0.0.0.0:0              LISTENING
TCP    0.0.0.0:445              0.0.0.0:0              LISTENING
TCP    127.0.0.1:1029           0.0.0.0:0              LISTENING
TCP    192.168.232.137:139     0.0.0.0:0     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

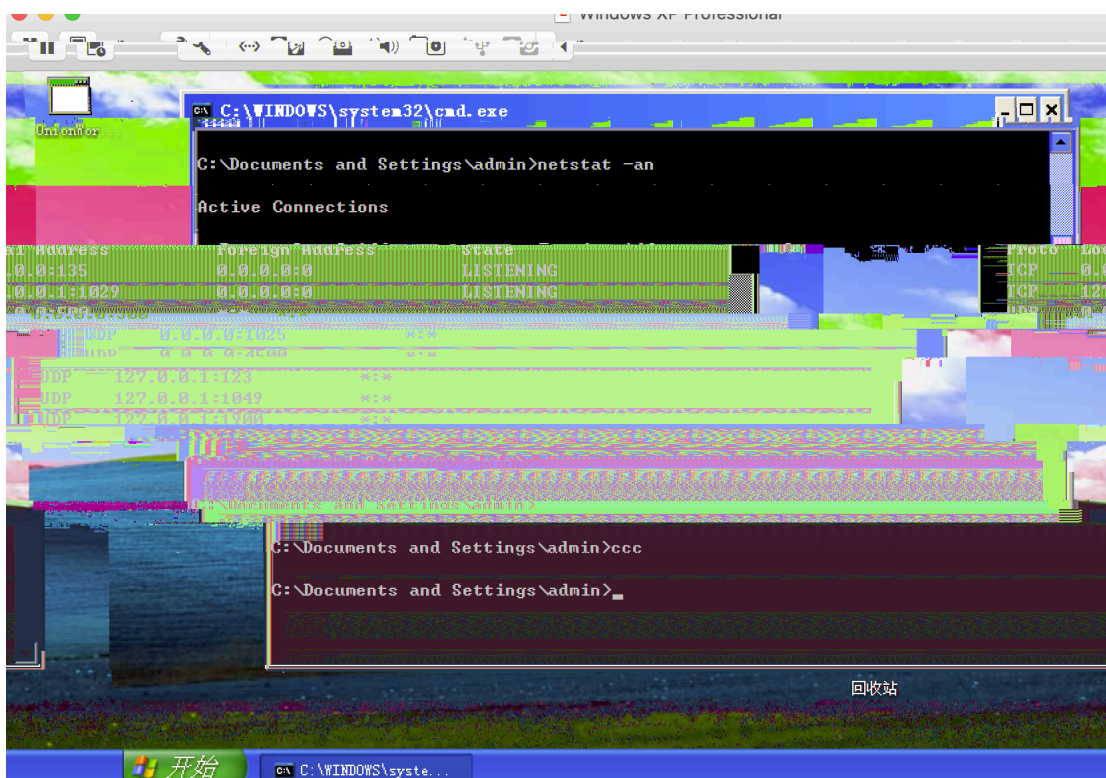
入 net stop rdr

net stop srv

net stop netbt



再 入 netsta -an, 功关 445 。

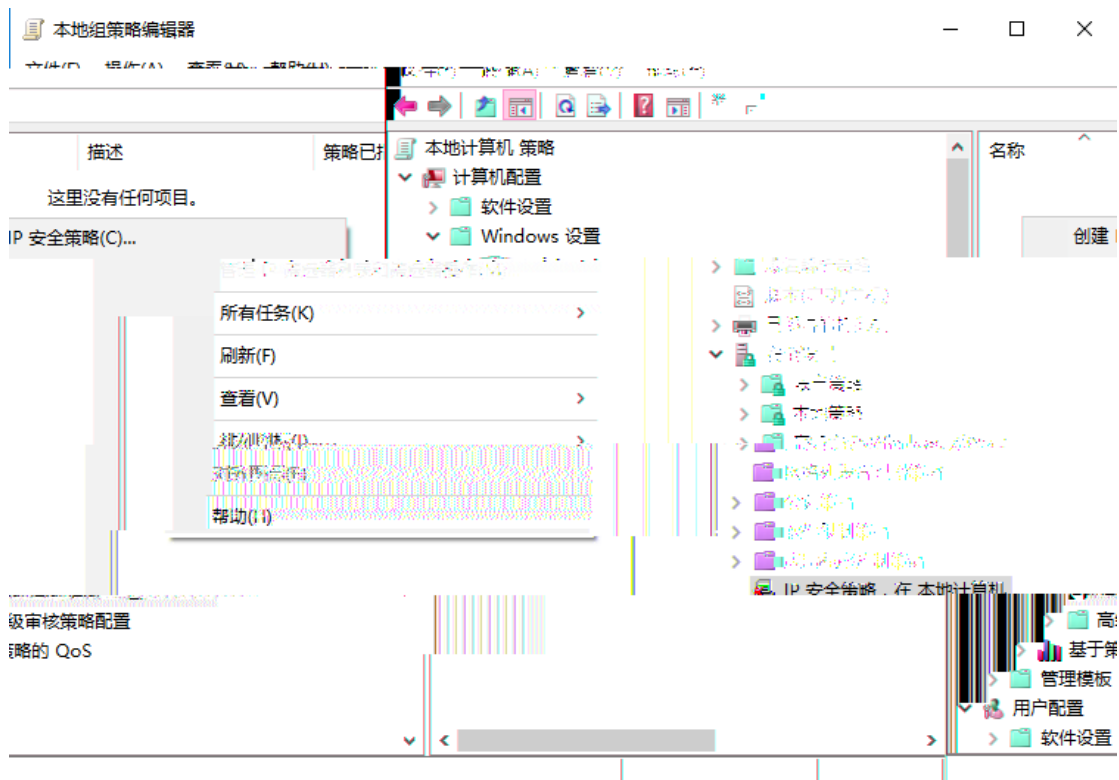


： 主 ACL 445

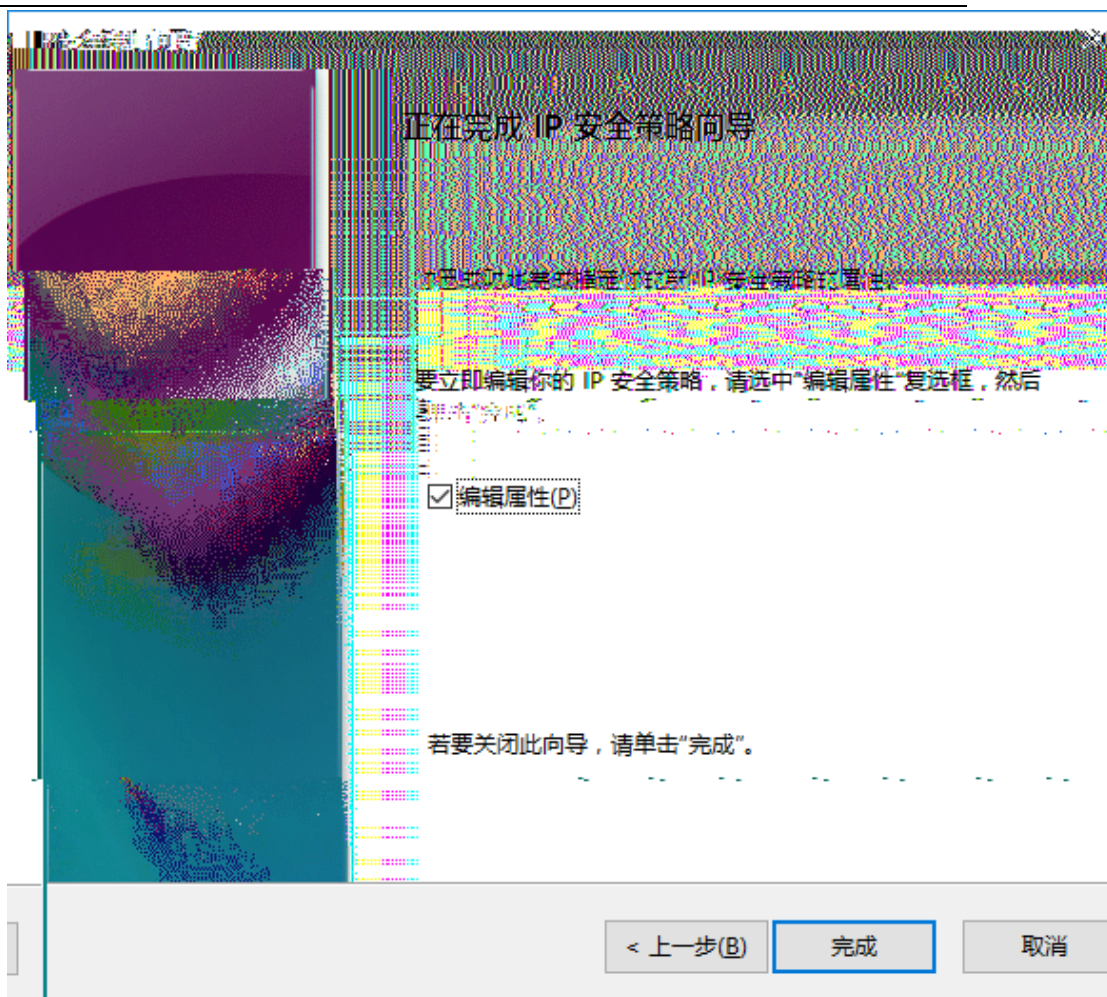
IP 全 制 Windows 共享协 关



单-> ， 入 gpedit.msc 。  
 中， ->windows -> 全 ->ip 全 下，  
 单击， “创 IP 全 ”

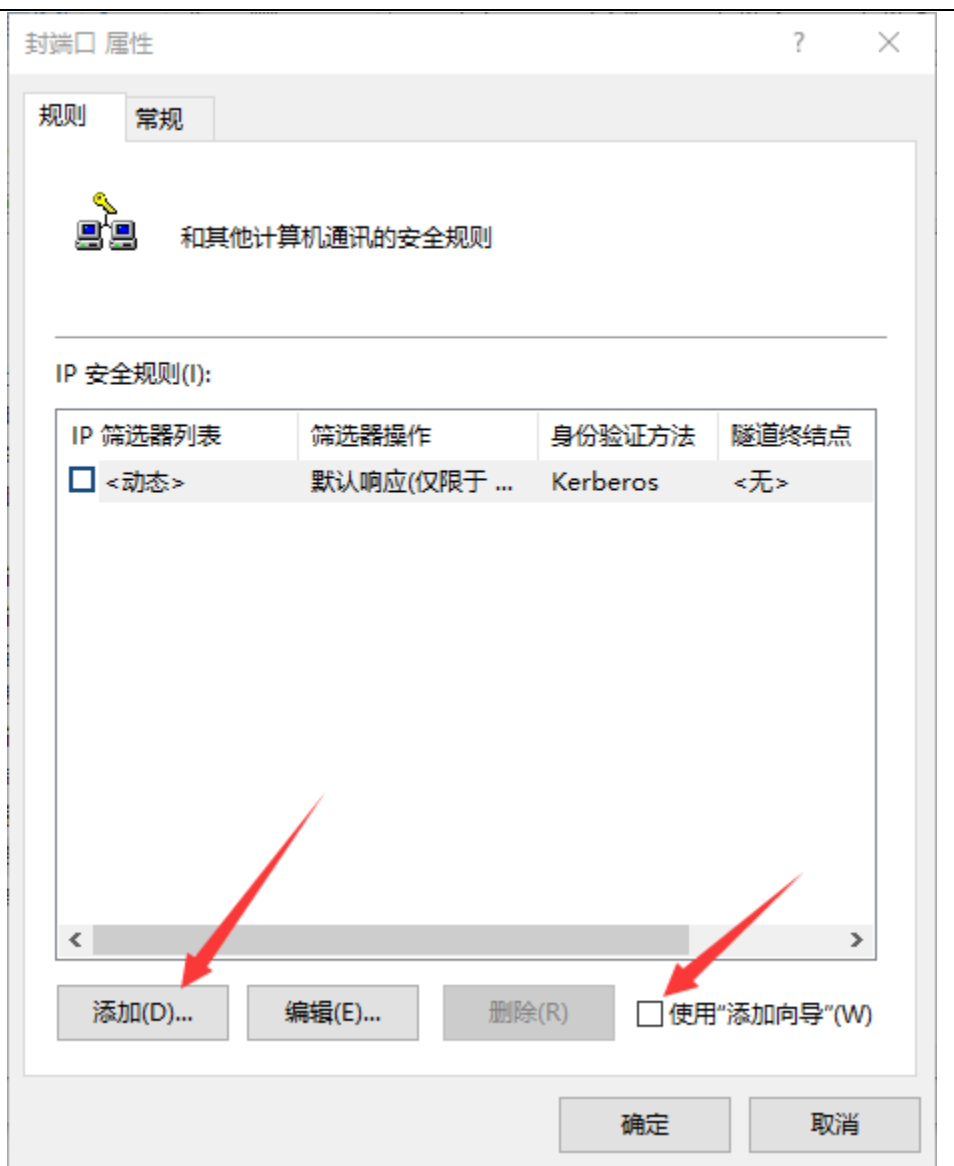


下一 -> 写 “ ”， 下一 ->下一 ->勾 ，

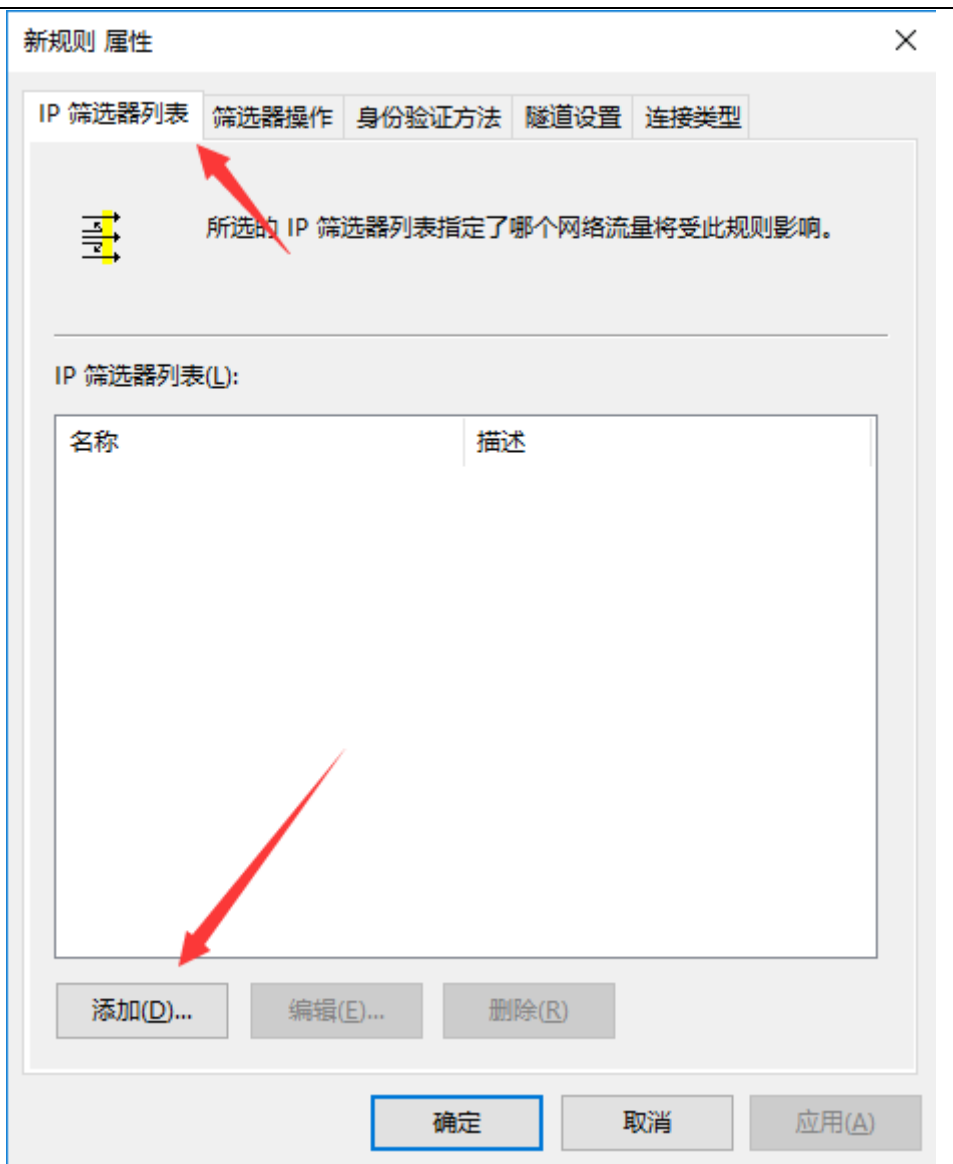


去 “使 加 ” 勾 ， 击 “ 加 ”

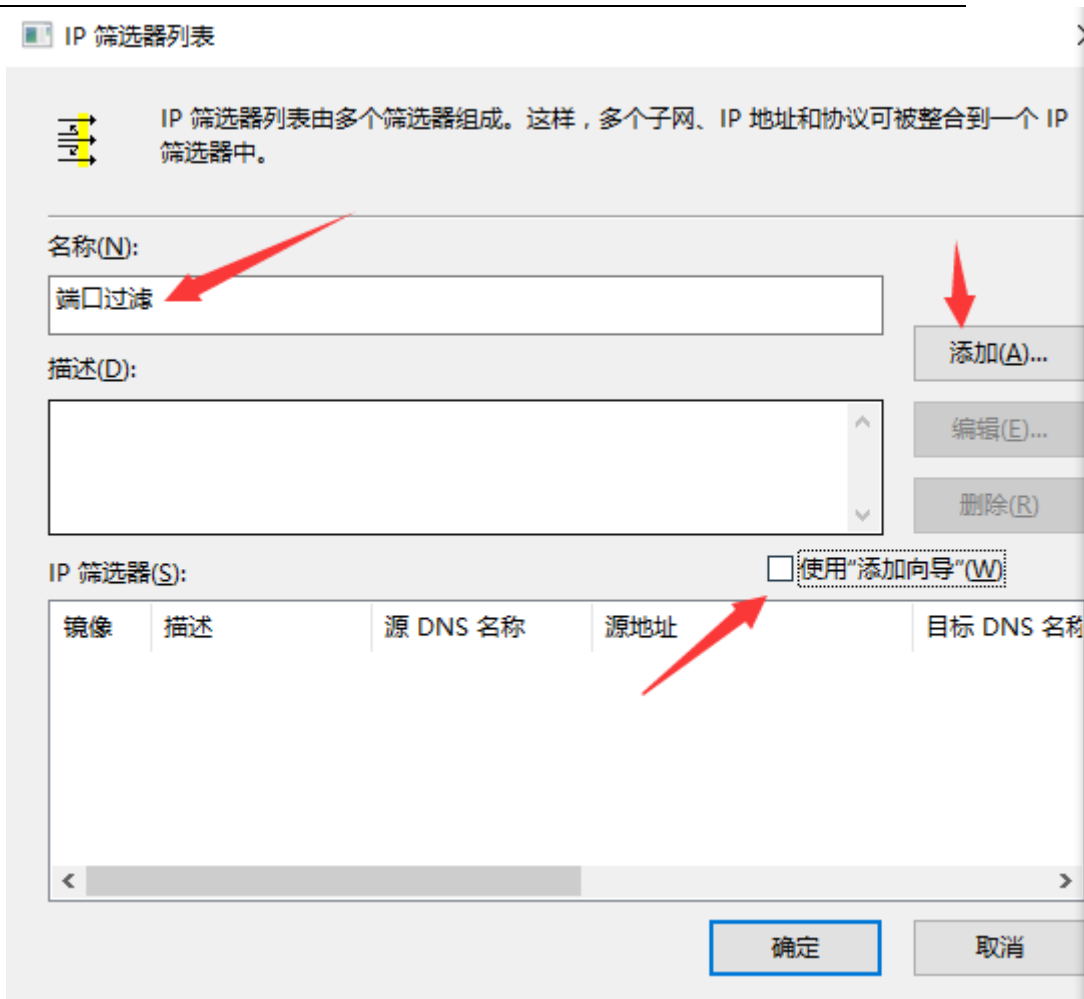




出， “IP 列” 卡， 击“加”

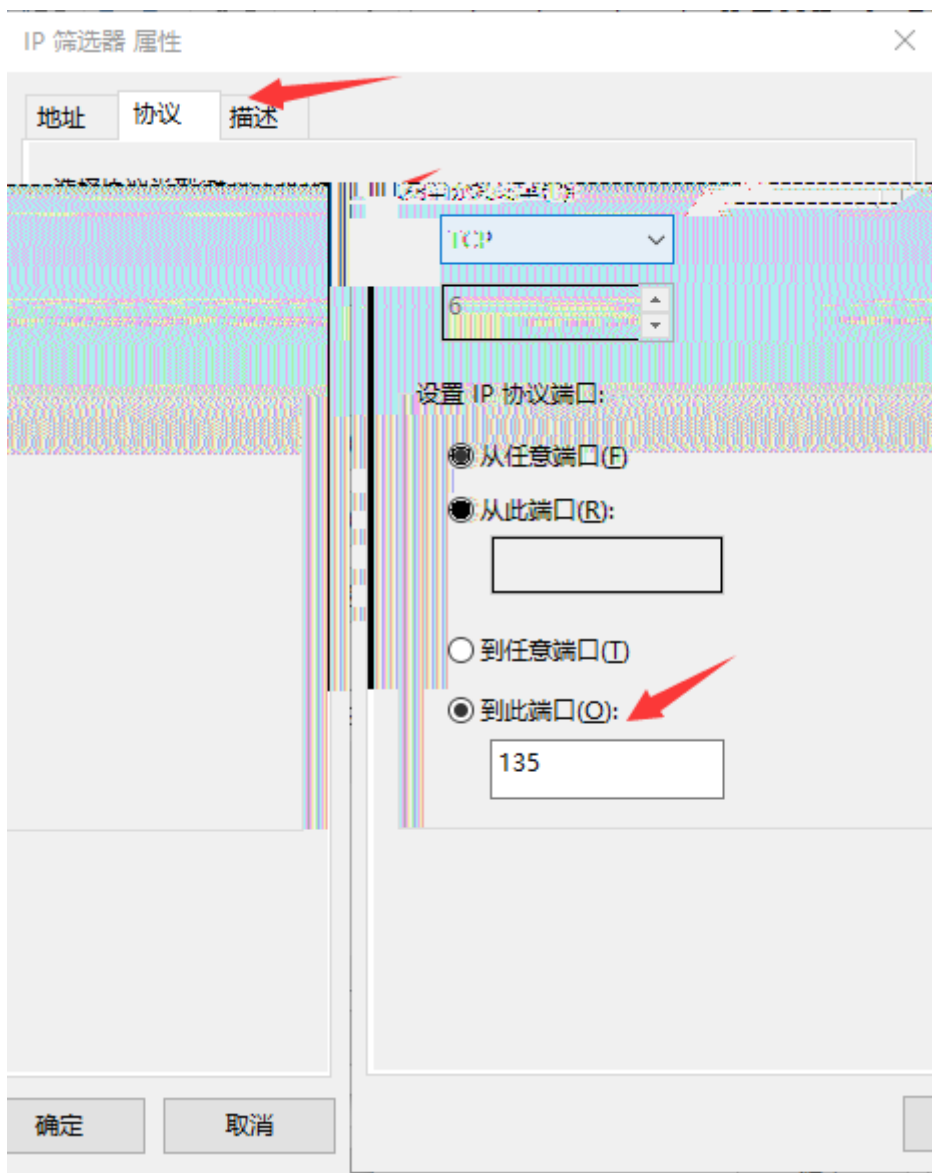


出 中 写 ，去 “使 加 ”前 勾，单击“ 加”

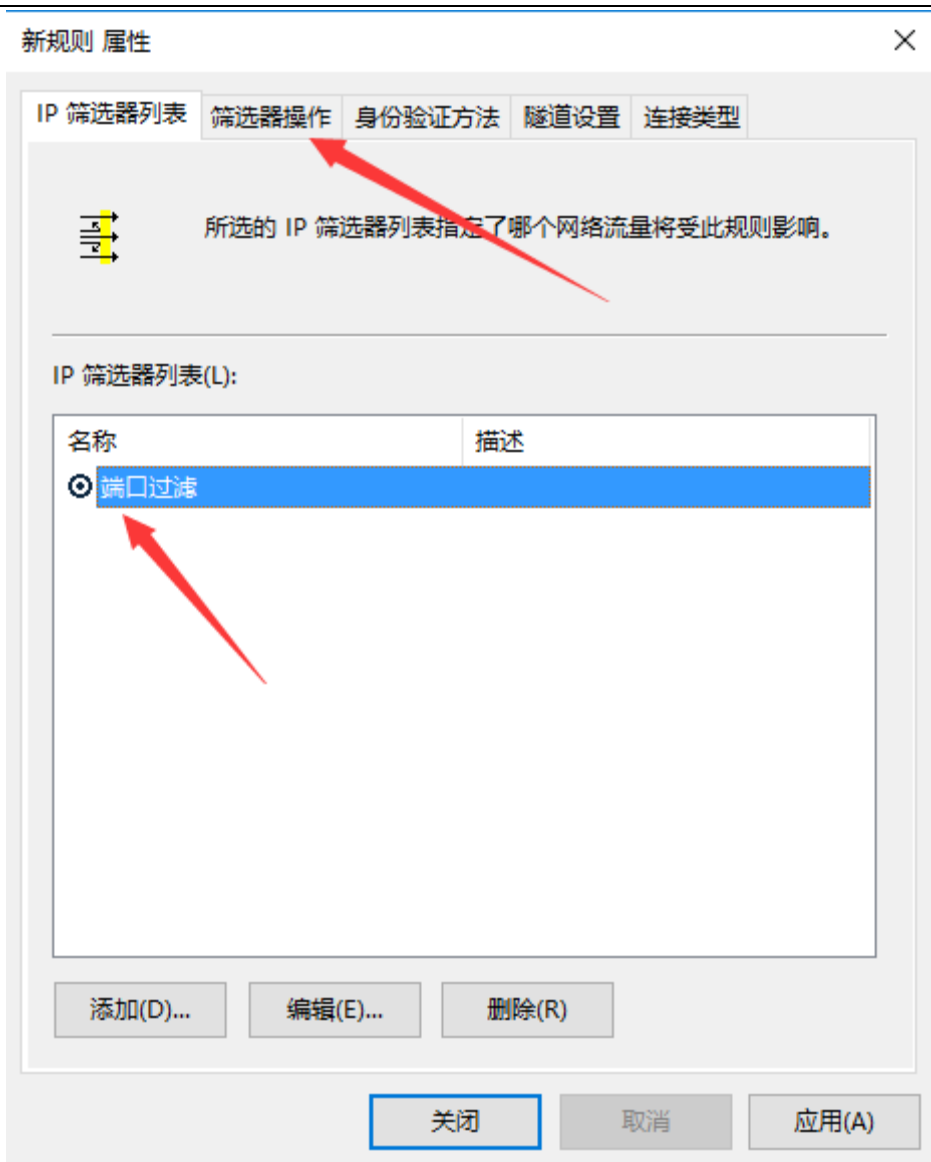


出 中，“协 ” 卡下， 协 到 信 ，

。

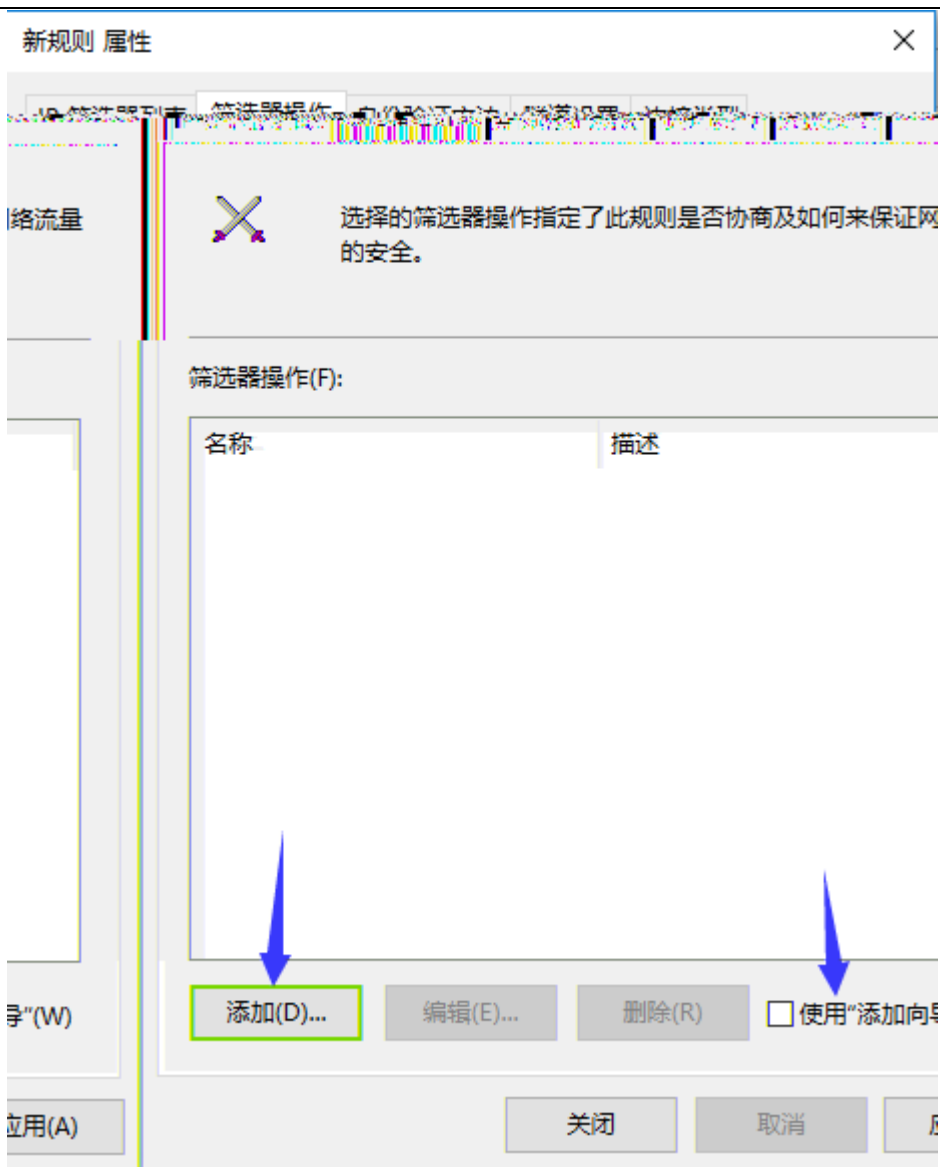


7 个 ， 加 TCP 135、139、445。 加 UDP 137、138。  
加全 ， 。  
中刚 加 “ ” 则， “ 作” 卡。



去 “使 加 ” 勾 ， 单击 “ 加 ”





1. “ ”

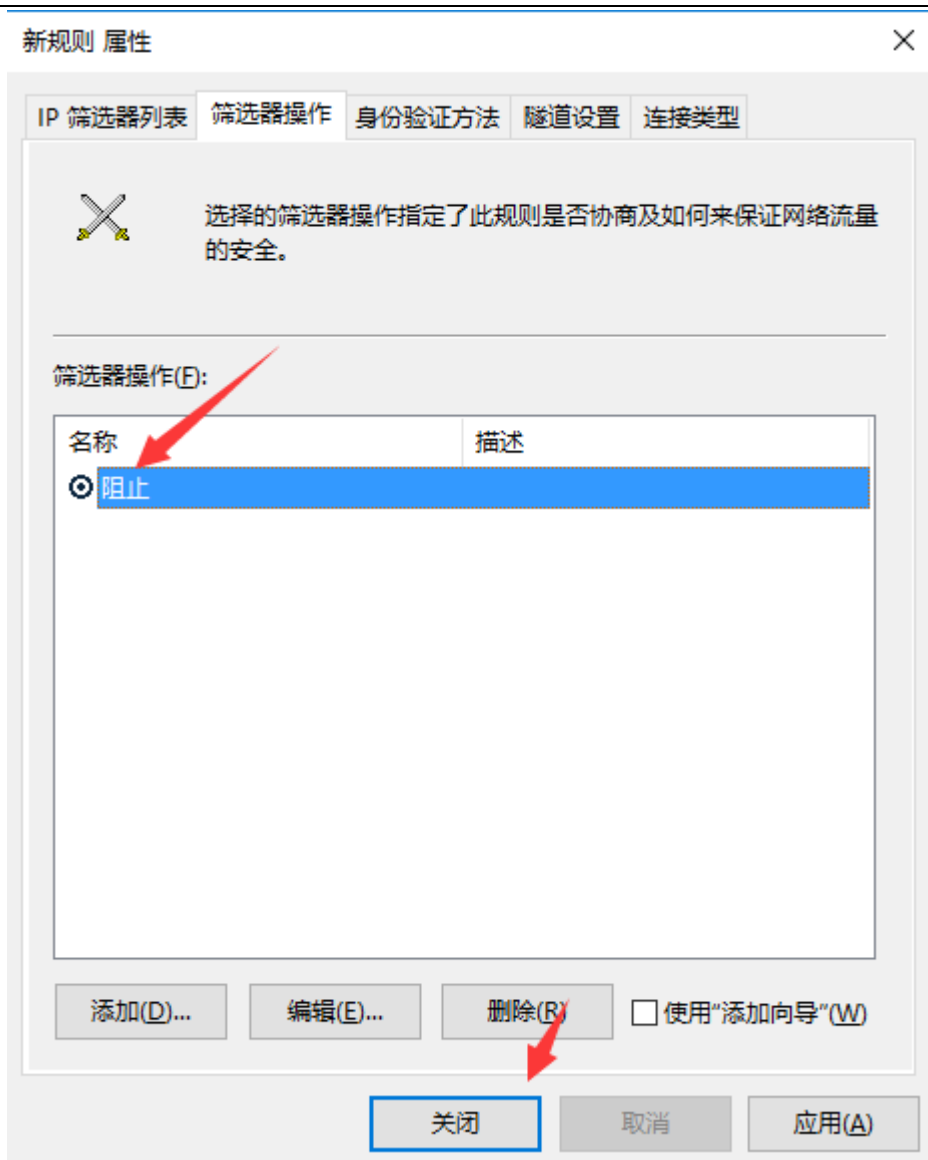


2. “ ” 卡， 个 “ ”， “ ”。

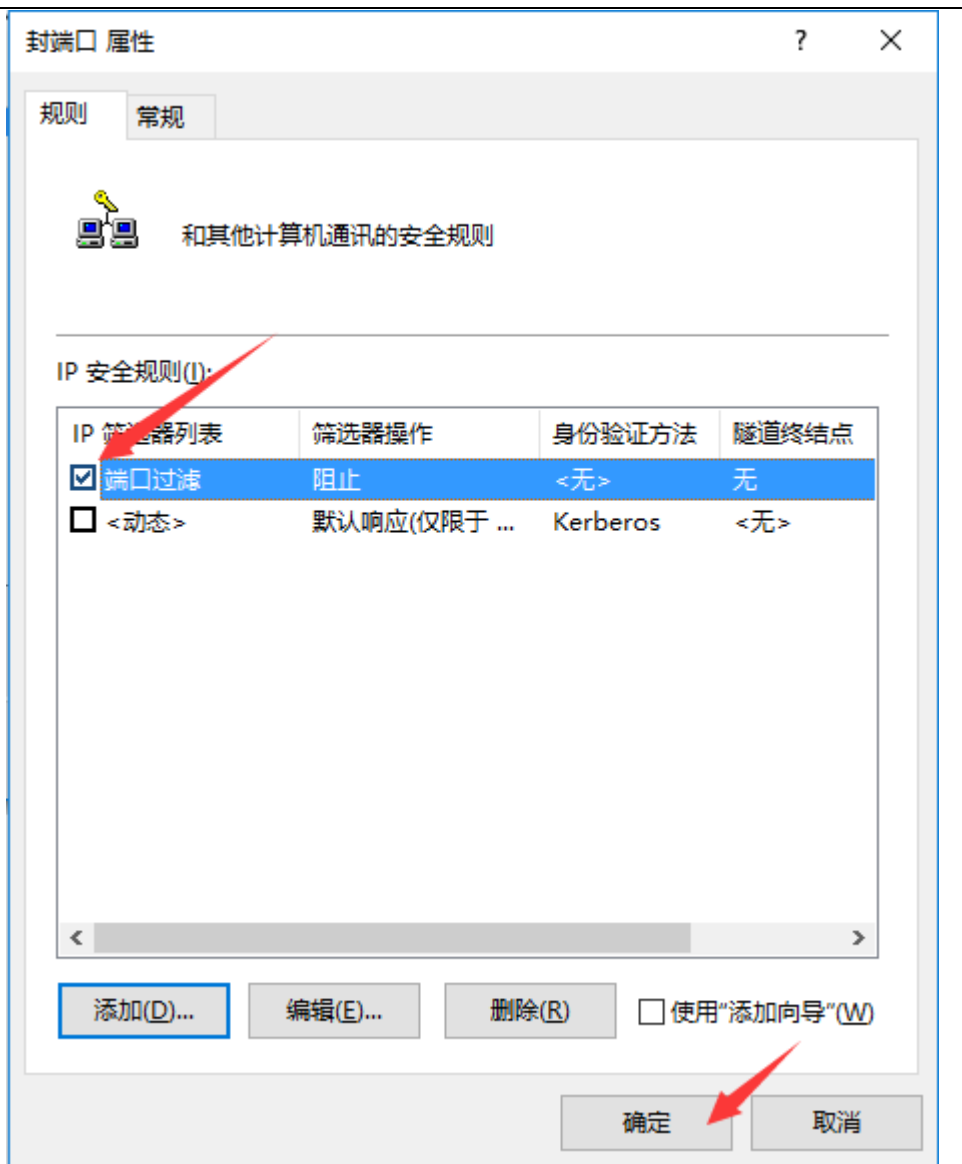
击

3. “IP 列 ” 卡下 “ ” 中。 “ 作”

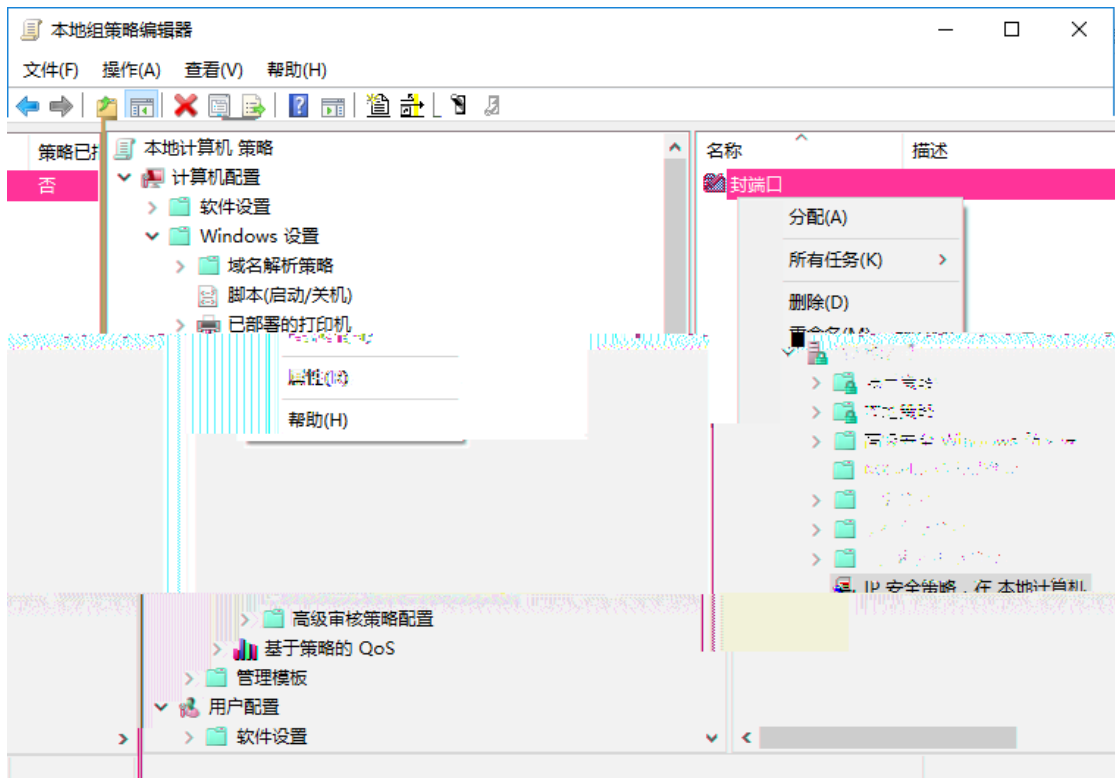
卡下 “ ” 中。 击“关 ”。



4. 全 则 。 击 。



5. “ ” 上， “分 ” ， 则 。





于众，为了免之传，利  
 ACL，以临。  
 主利TCP 445传，于企事业单位  
 。为了传，三位，ACL  
 则从TCP 445。  
 以下内于为，举例何ACL则，以  
 TCP 445传，仅供。作中，协人  
 厂务人，上。

### Juniper (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
```

# 全 则

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

# 三 则

```
set interfaces [ 三 ] unit 0 family inet filter output
deny-wannacry
set interfaces [ 三 ] unit 0 family inet filter input
deny-wannacry
```

---

华三(H3C) ( 例) :

```

:
acl number 3050
rule deny tcp destination-port 445
rule permit ip

interface [      三      ]
packet-filter 3050 inbound
packet-filter 3050 outbound

:
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

# 全
qos apply policy deny-wannacry global inbound
qos apply policy deny-wannacry global outbound

# 三      则
```

---

```
interface [          三          ]  
qos apply policy deny-wannacry inbound  
qos apply policy deny-wannacry outbound
```

**华为** ( 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 [          三          ]  
    traffic-policy deny-wannacry inbound  
    traffic-policy deny-wannacry outbound
```

**Cisco** ( 例 ) :

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

```
interface [ 三 ]
```

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

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

```
:
```

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

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

```
permit ip any any
```

```
interface [ 三 ]
```

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

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

( 例 ) :

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

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

```
permit ip any any
```

```
interface [ 三 ]
```

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

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

## 第3章 互 主 作 南

， 使 360 全卫 “NSA 免 具”，  
一 修 、关 务，包 准 出 NSA 使

修， 丁。 XP、2003 丁  
， 具 助 关 危 务，从 NSA  
击 “免 ”。  
NSA 免 具下 : <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)
- 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