**针对“永恒之蓝”攻击紧急处置手册**

**（蠕虫WannaCry）**



**2017年05月13日**

目录

[第1章 隔离网主机应急处置操作指南 3](#_Toc482455350)

[首先确认主机是否被感染 3](#_Toc482455351)

[方式一：启用蠕虫快速免疫工具 4](#_Toc482455352)

[方式二：针对主机进行补丁升级 4](#_Toc482455353)

[方式三：关闭445端口相关服务 5](#_Toc482455354)

[方式四：配置主机级ACL策略封堵445端口 6](#_Toc482455355)

[第2章 核心网络设备应急处置操作指南 19](#_Toc482455356)

[Juniper设备的建议配置（示例）: 19](#_Toc482455357)

[华三(H3C)设备的建议配置（示例）: 20](#_Toc482455358)

[华为设备的建议配置（示例）: 21](#_Toc482455359)

[Cisco设备的建议配置（示例）: 21](#_Toc482455360)

[锐捷设备的建议配置（示例）: 22](#_Toc482455361)

[第3章 互联网主机应急处置操作指南 22](#_Toc482455362)

# 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。**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。

## 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（**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/

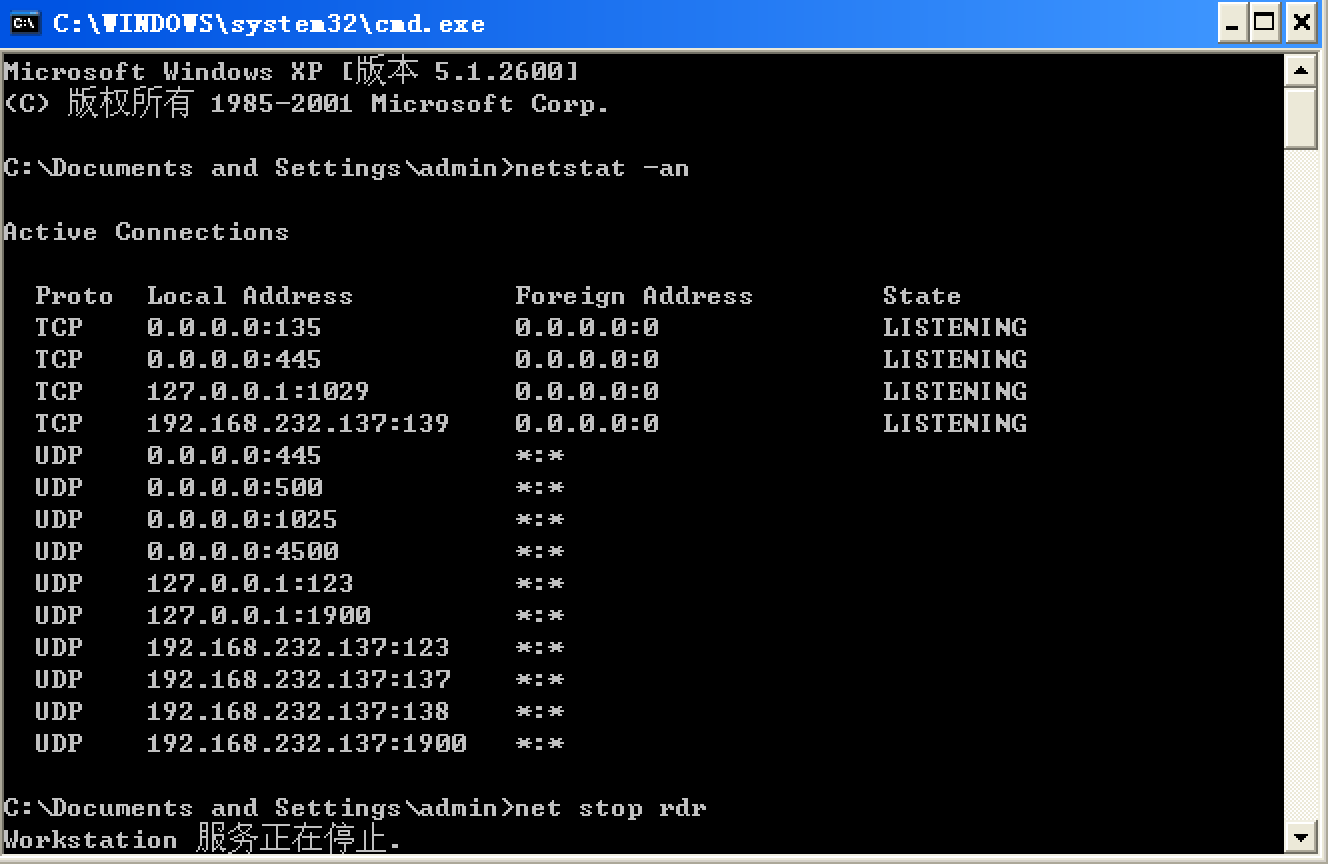
快速下载地址：

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

## 方式三：关闭445端口相关服务

点击开始菜单，运行，cmd，确认。

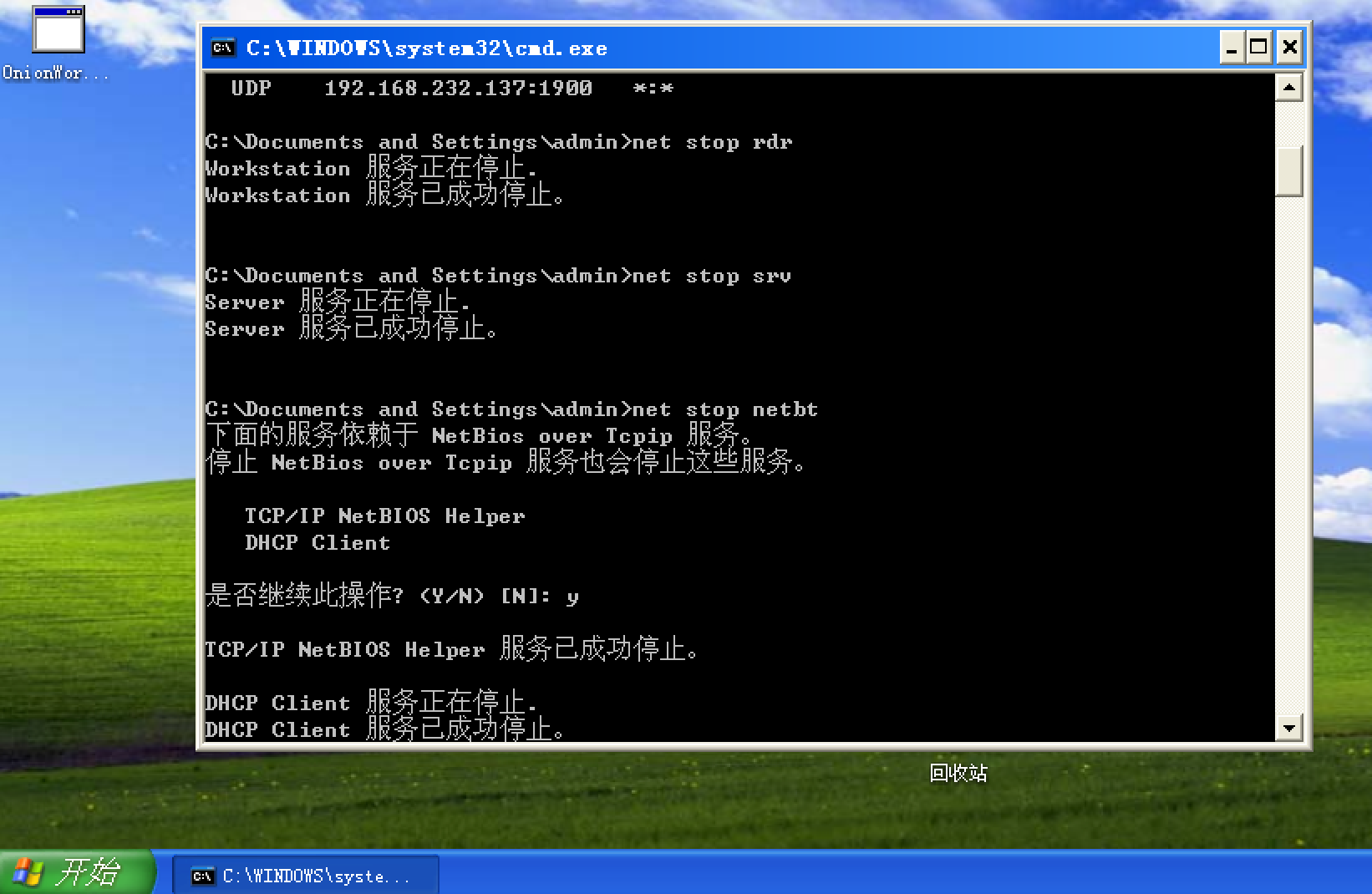
输入命令netstat –an查看端口状态



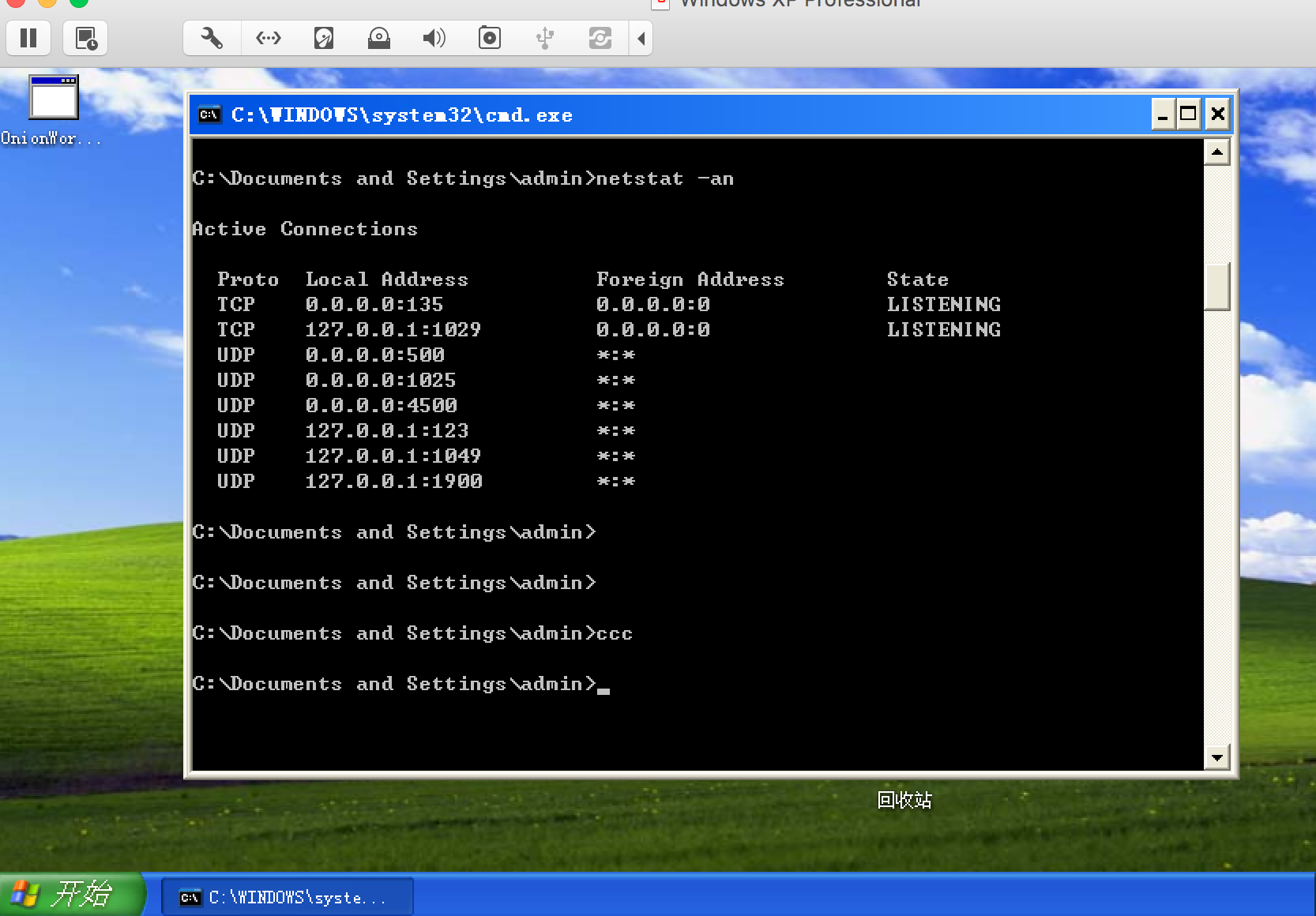
输入net stop rdr 回车

net stop srv 回车

net stop netbt 回车



再次输入netsta –an，成功关闭445端口。

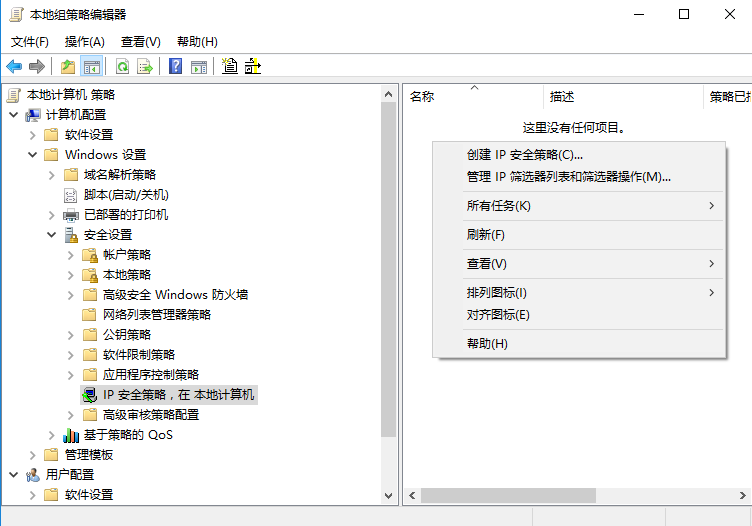


## 方式四：配置主机级ACL策略封堵445端口

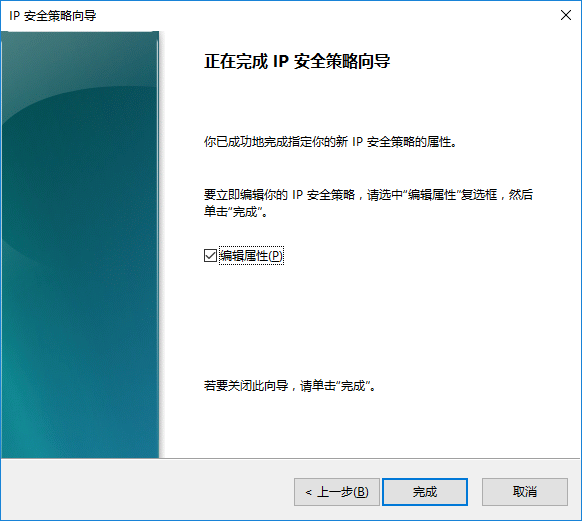
通过组策略IP安全策略限制Windows网络共享协议相关端口

开始菜单->运行，输入gpedit.msc回车。打开组策略编辑器

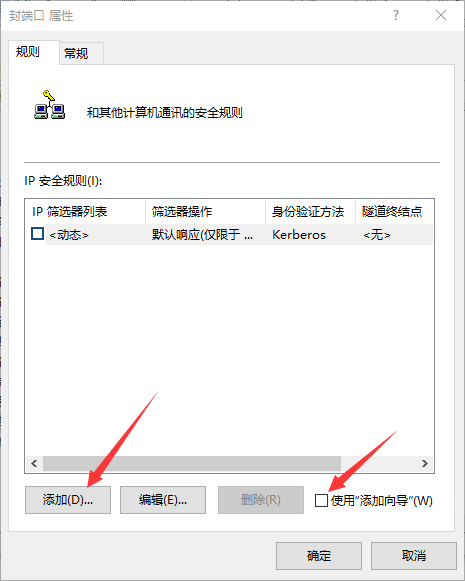
在组策略编辑器中，计算机配置->windows设置->安全设置->ip安全策略 下，在编辑器右边空白处鼠标右键单击，选择“创建IP安全策略”



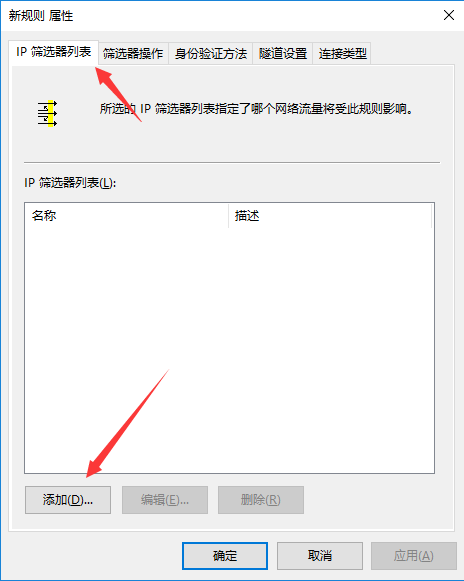
下一步->名称填写“封端口”，下一步->下一步->勾选编辑属性，并点完成



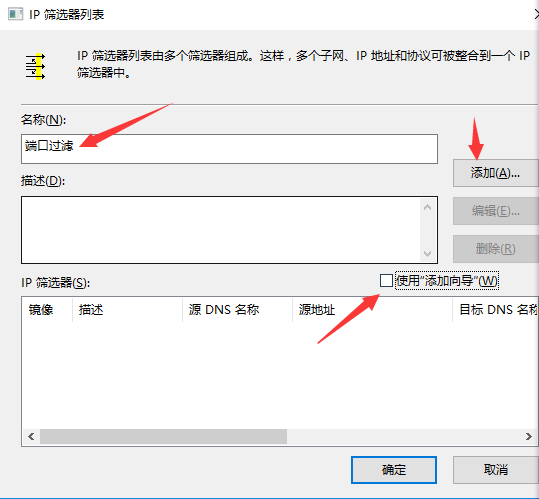
去掉“使用添加向导”的勾选后，点击“添加”



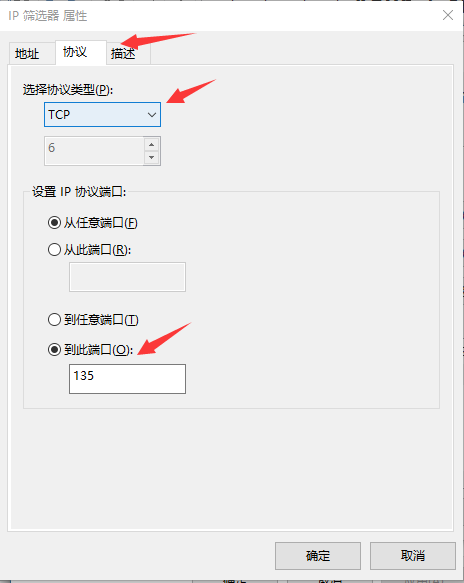
在新弹出的窗口，选择“IP筛选列表”选项卡，点击“添加”



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”

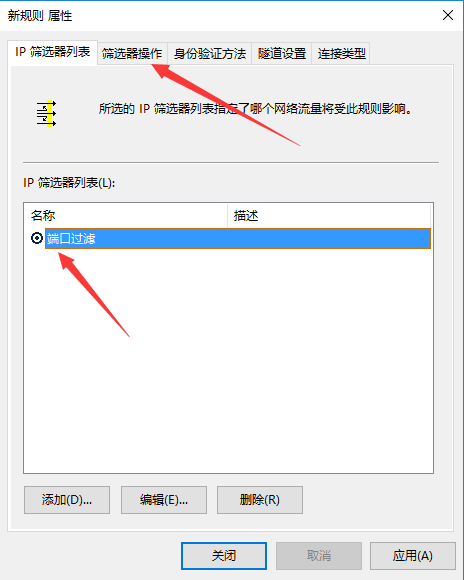


在新弹出的窗口中，“协议”选项卡下，选择协议和设置到达端口信息，并点确定。

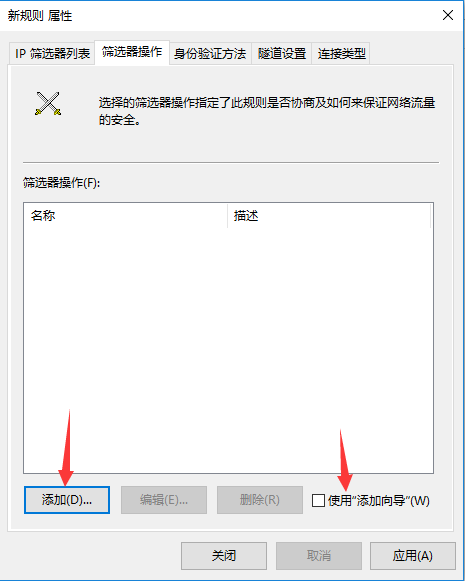


重复第7个步骤，添加TCP端口135、139、445。添加UDP端口137、138。添加全部完成后，确定。

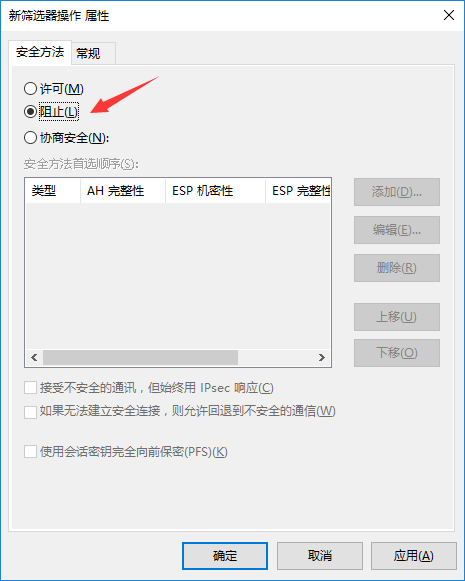
选中刚添加完成的“端口过滤”规则，然后选择“筛选器操作”选项卡。



去掉“使用添加向导”勾选，单击“添加”按钮



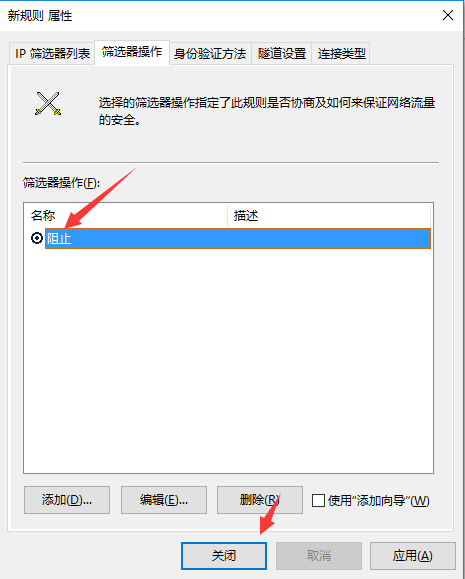
1. 选择“阻止”



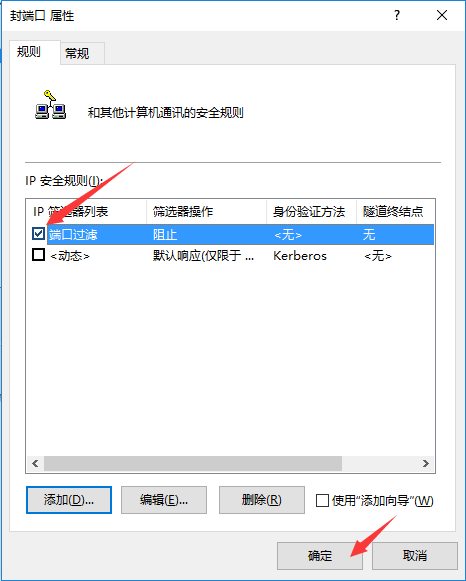
1. 选择“常规”选项卡，给这个筛选器起名“阻止”，然后“确定”。

点击

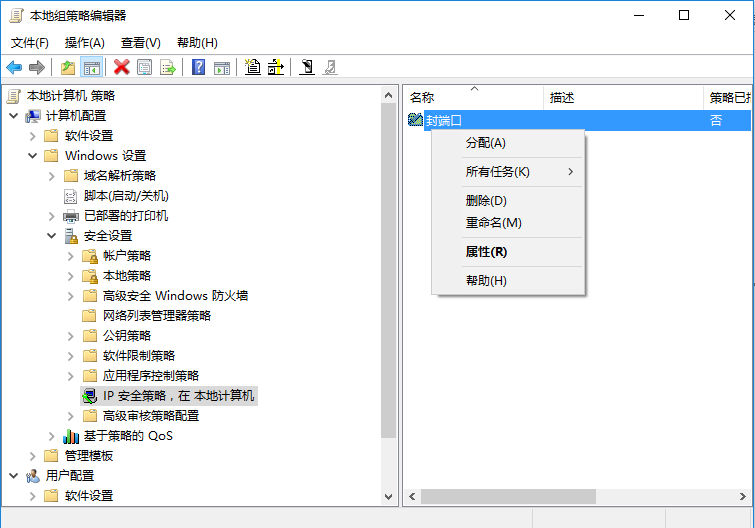
1. 确认“IP筛选列表”选项卡下的“端口过滤”被选中。确认“筛选器操作”选项卡下的“阻止”被选中。然后点击“关闭”。



1. 确认安全规则配置正确。点击确定。



1. 在“组策略编辑器”上，右键“分配”，将规则启用。



# 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进行配置。

## 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

# 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>

