360 虚拟化安全产品

-“永恒之蓝”应急响应方案

2017 年 05 月 12 日

1. 漏洞描述

1.1 漏洞描述

2017 年 5 月 12 日起，在国内外网络中发现爆发基于 Windows 网络共享协议进行攻击传播的蠕虫恶意代码，这是不法分子通过改造之前泄露的 NSA 黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件。

目前发现的蠕虫会扫描开放 445 文件共享端口的 Windows 机器，无需用户任何操作，只要开机上网，不法分子就能在电脑和服务器中植入执行勒索程序、远程控制木马、虚拟货币挖矿机等恶意程序。

此蠕虫目前在没有对 445 端口进行严格访问控制的教育网、企业内网及业务外网大量传播，呈现爆发的态势，受感染系统会被勒索高额金钱，不能按时支付赎金的系统会被销毁数据造成严重损失。该蠕虫攻击事件已经造成非常严重的现实危害，各类规模的网络也已经面临此类威胁。

1.2 影响范围

涉及开放 445 SMB 服务端口且没有及时安装安全补丁的客户端和服务器系统都将可能面临此威胁。

1.3 建议处置办法

- 已购买我司虚拟化安全产品客户，建议立即配置防火墙相关策略；如未购买防火墙模块，可致电 360 服务热线：400-136-360 获取帮助。
- 对于 Win7 及以上版本的操作系统，微软已发布补丁 MS17-010 修复了“永恒之蓝”攻击的系统漏洞，请立即安装此补丁。

  补丁地址：https://technet.microsoft.com/zh-cn/library/security/MS17-010

2. 应急方案 – 已购买防火墙模块的用户

对于 Win7 及以上版本的系统确认是否安装 MS17-010 补丁，如果没有安装则受威胁影响；Win7 以下的 Windows XP/2003 没有补丁，只要开启 SMB 服务就会受到影响。

为了减少“永恒之蓝”带来的损失，我们建议客户首先对向外开放的 445 等共享端口进行防火墙阻断控制，并及时部署 MS17-010 补丁，同时升级 IPS、应用识别等设备的特征库。

提醒：执行应急处置办法之前，请管理员先自行评估关闭 135、137、138、139、445 端口对业务是否带来影响。

2.1 适用于以下虚拟化安全产品

版本
360 虚拟化安全管理系统 v6.0（轻代理型）
360 虚拟化安全管理系统 v6.1（轻代理型）
360 虚拟化安全管理系统 v7.0（轻代理型）
360 虚拟化安全管理系统 v6.1（无代理型）

2.2 360 虚拟化安全管理系统 v6.x（轻代理型）

在虚拟化安全 V6.x 版本控制中心，点击【策略】-【防火墙策略】-【策略模板】，新建策略模板 SMB。

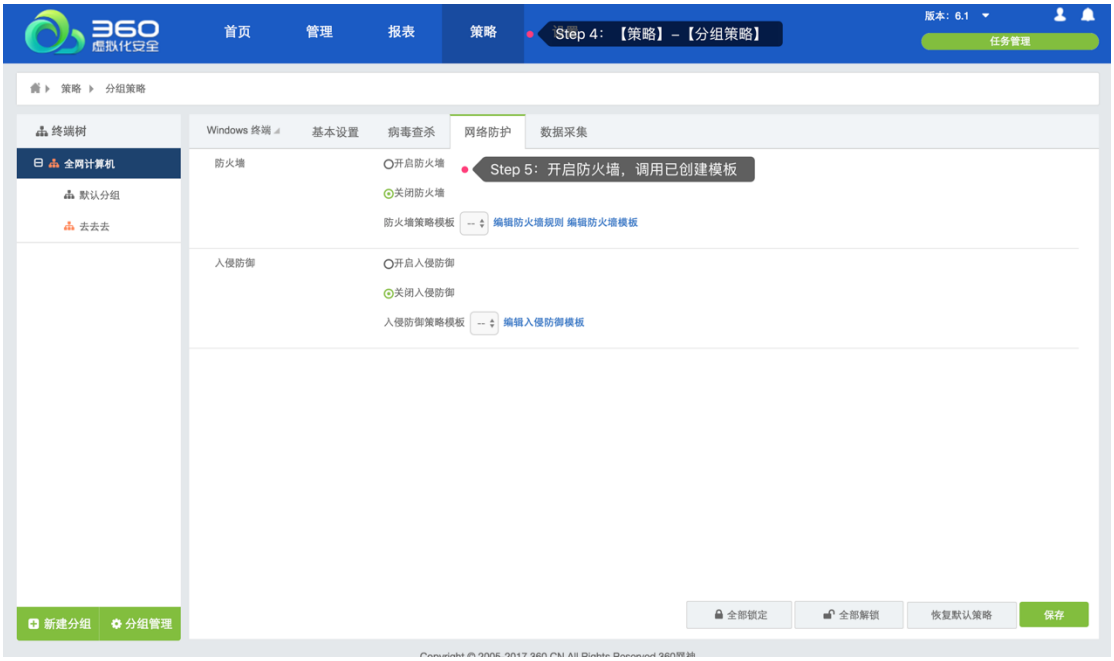
在【防火墙策略】-【防火墙规则】中新建规则。

配置参数：

- 优先级：建议最高
- 流向：设定为流入
- 协议：TCP
- 端口：135、137、138、139、445
- 远端 IP：任意
- 远端端口：任意

进入【策略】-【分组策略】-【网络防护】，开启防火墙功能，并引用刚才创建的防火墙模板。

点击保存，并执行生效。

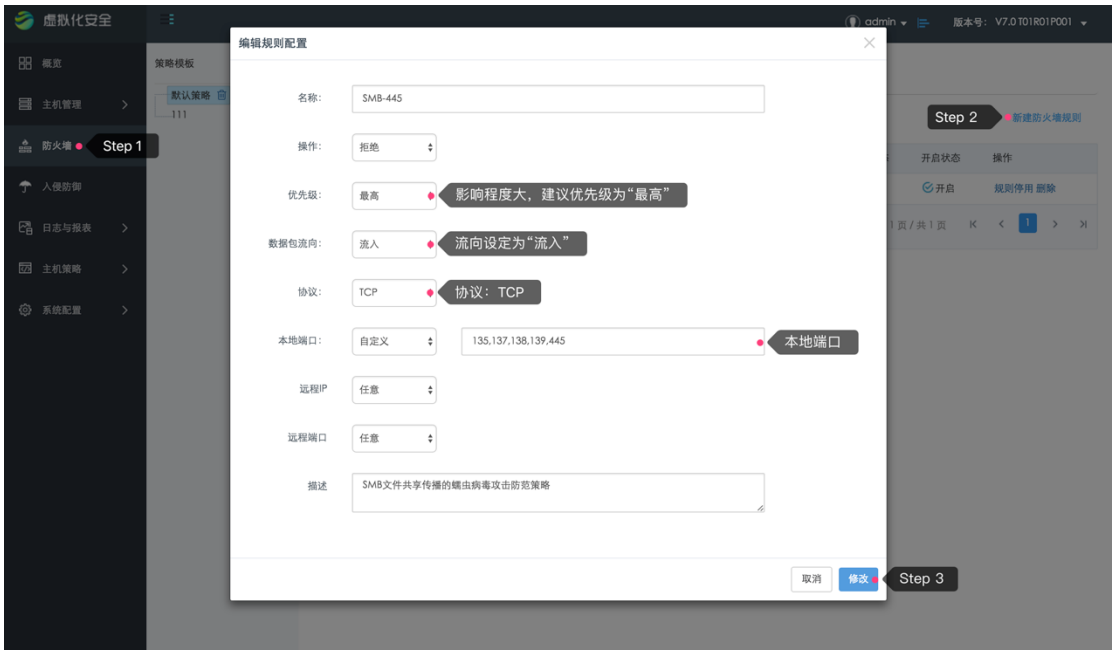


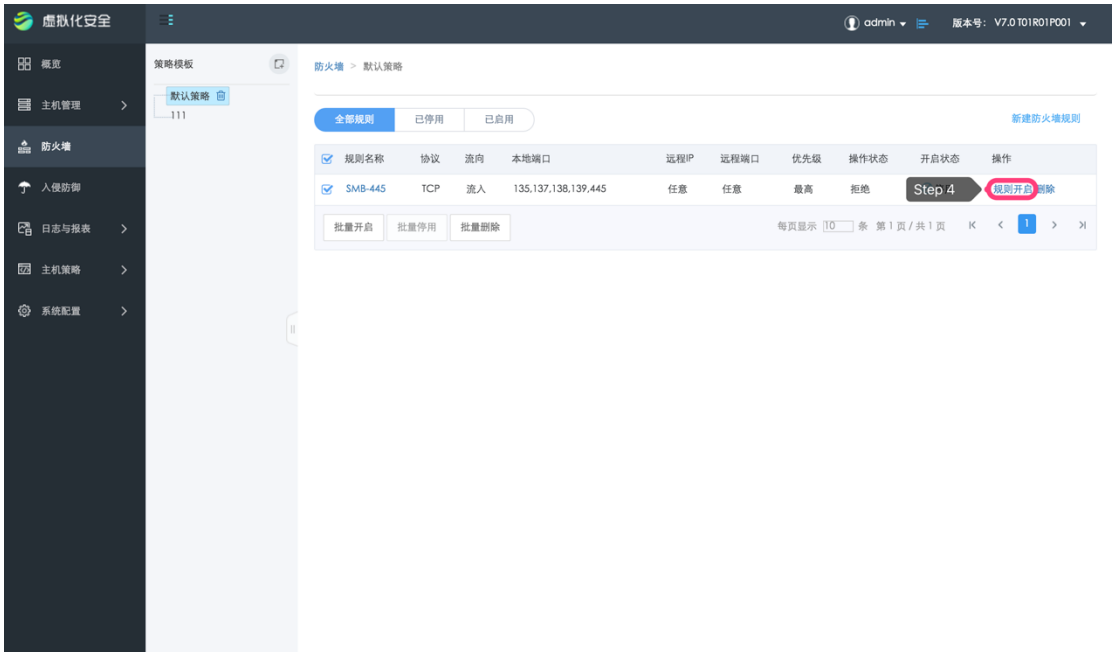
2. 3 360 虚拟化安全管理系统 v7.x（轻代理型）

在虚拟化安全 V7.x 版本控制中心，点击【防火墙】”，新建策略模板 SMB，并选择“新建防火墙配置”。

配置参数：

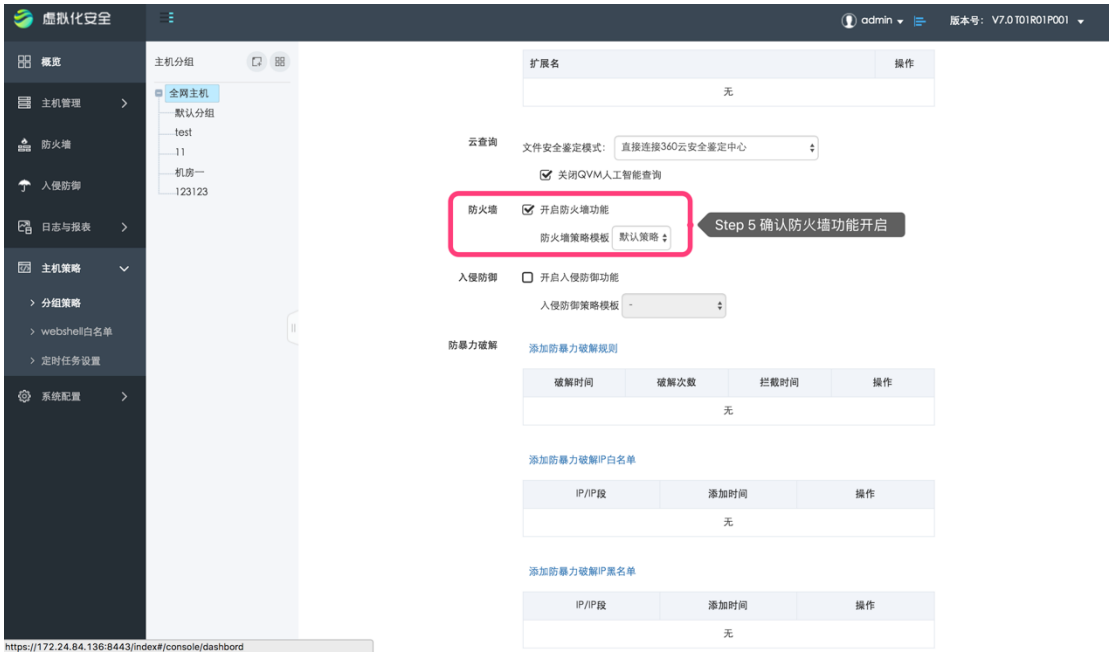
- 优先级：建议最高
- 流向：设定为流入
- 协议：TCP
- 端口：135、137、138、139、445
- 远端 IP：任意
- 远端端口：任意





设置好策略好，将规则开启。

并到【主机策略】-【分组策略】中确认防火墙功能是否开启，将防火墙策略模板调整到 SMB 策略模板即可完成应急处置。



2. 4 360 虚拟化安全管理系统 v6.1（无代理型）

在虚拟化安全 V6.1 无代理版本控制中心，点击【安全策略】-【安全配置】”，新建安全配置。

点击【新建防火墙规则】

配置参数：

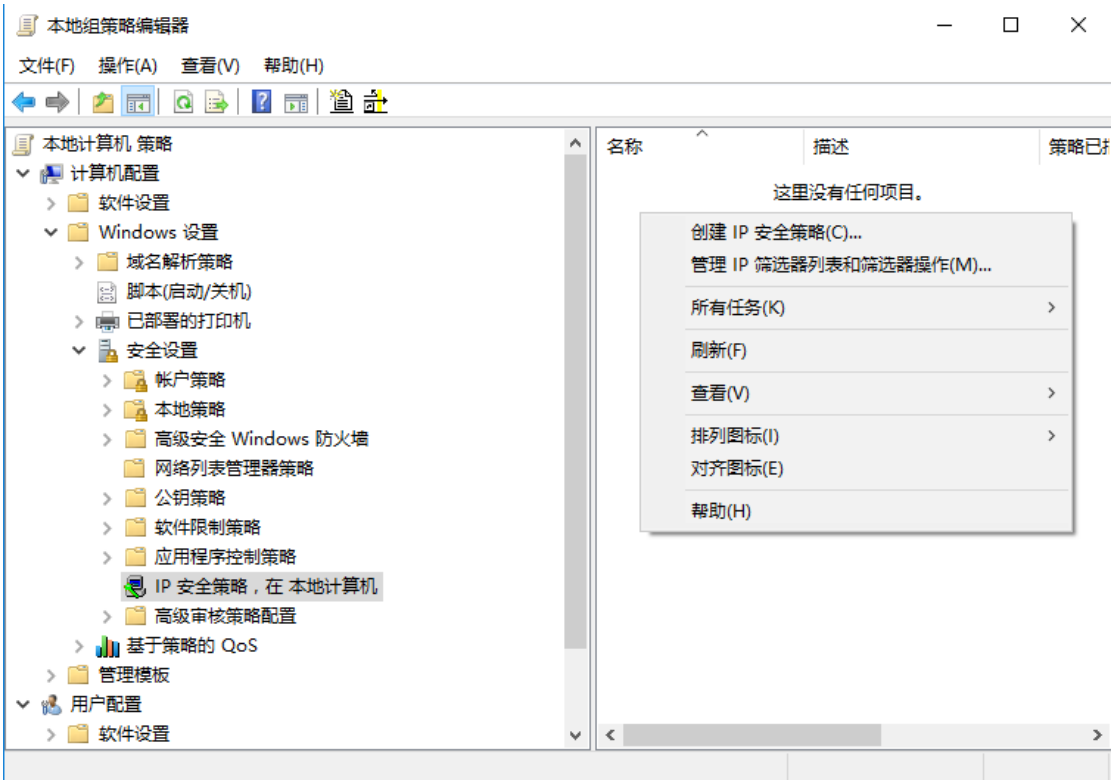
- 方向：设定为入站
- 动作：组织
- 协议：TCP
- 本地 IP 信息
- 本地端口信息：135、137、138、139、445
- 远端 IP 信息：所有
- 远端端口信息：所有

设置完防火墙规则后，点击“确定”。并调整优先级为置顶，最后点击“保存”。


360 虚拟化安全
admin
注销
实时监控
警报
计算机
安全策略
分析
报表
管理
安全策略 > 安全配置
帮助
通用设置
防恶意软件
防火墙
应用程序控制
入侵防御
高级防护
新增
复制
删除
调整优先级
搜索:
名字
置顶
上移
下移
置底
Step 4：置顶该条策略
本地端口
远程IP地址
远程端口
SMB端口阻断
TCP
所有地址
135, 137, 138, 139, 445
所有地址
所有端口
从 1 到 1 /共 1 条规则
保存
Step 5：保存

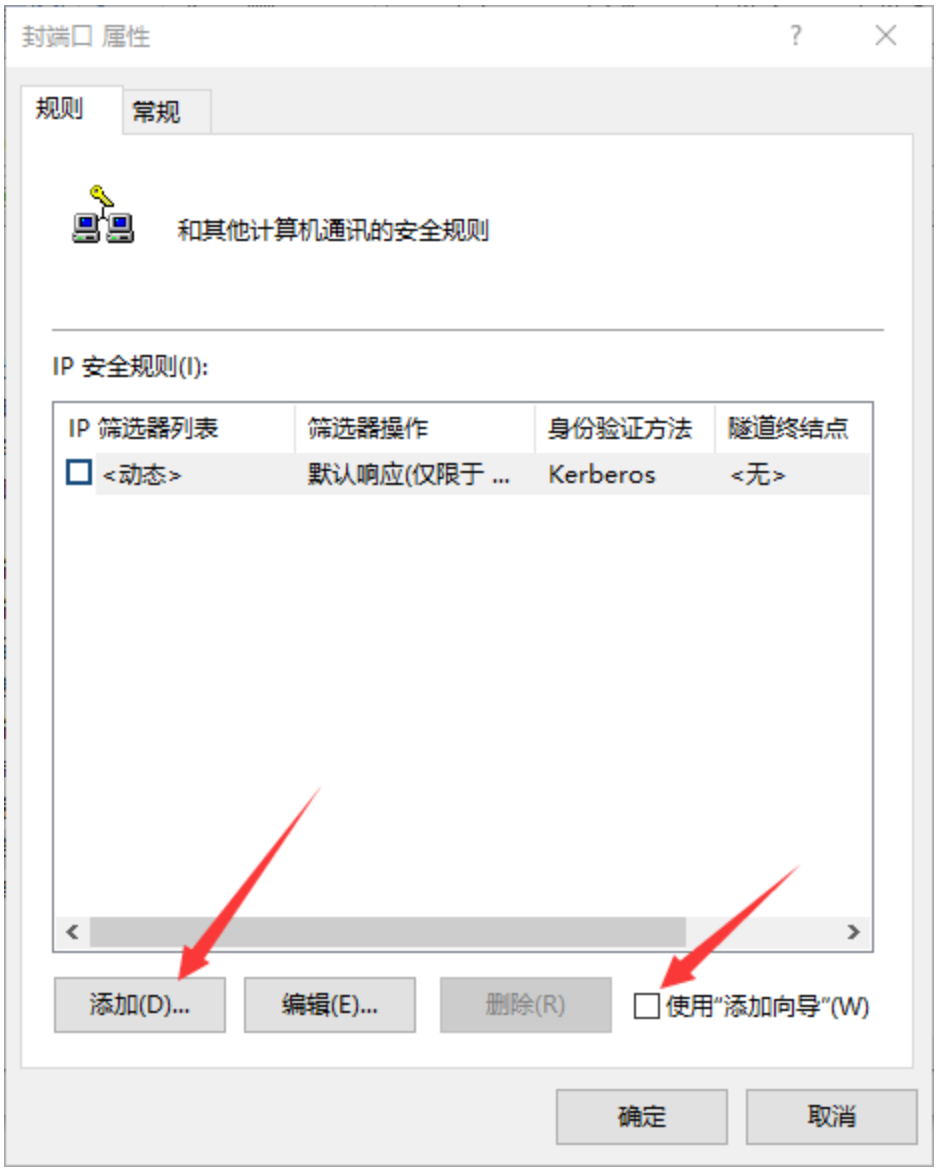
3. 应急方案 – 未购买防火墙模块的用户

1. 开始菜单->运行，输入 gpedit.msc 回车。打开组策略编辑器
2. 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”

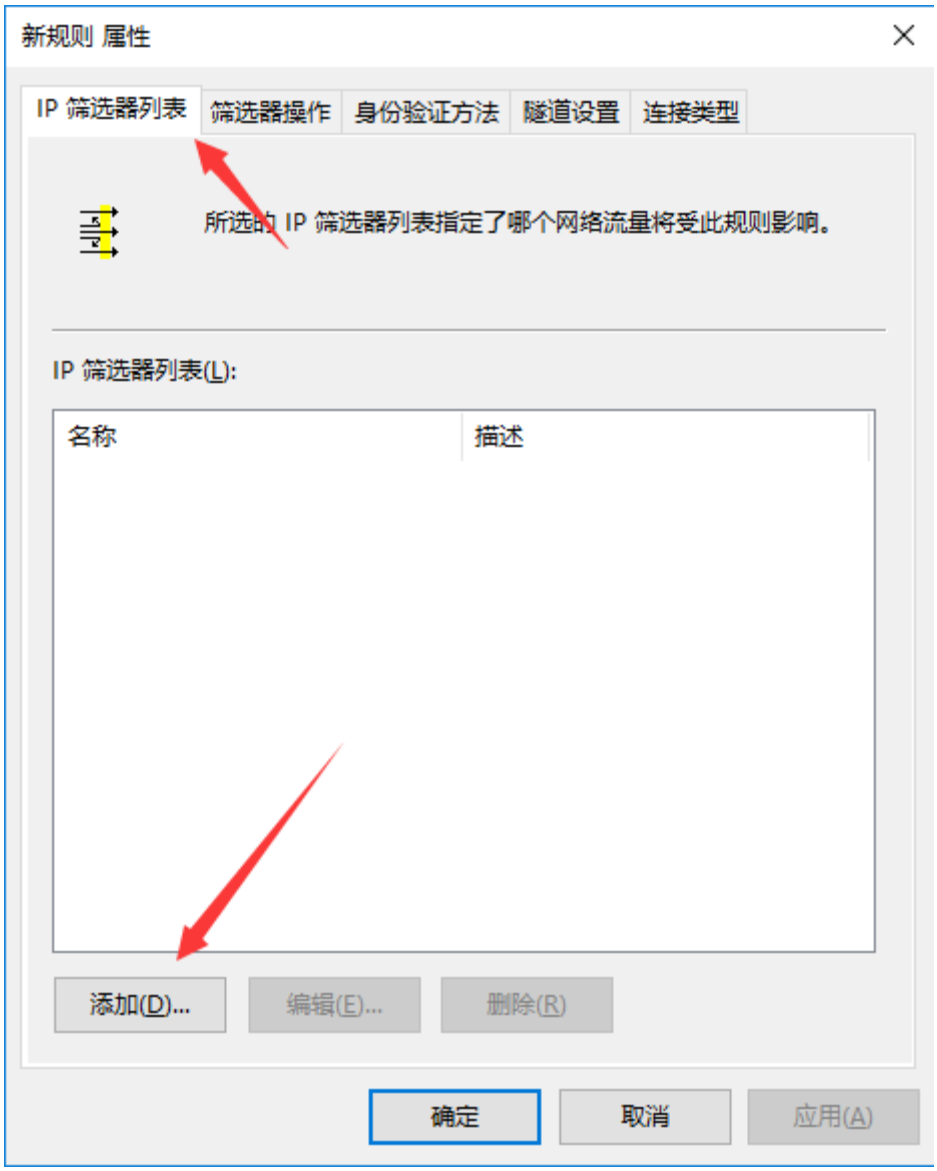


3. 下一步->名称填写“封端口”，下一步->下一步->勾选编辑属性，并点完成

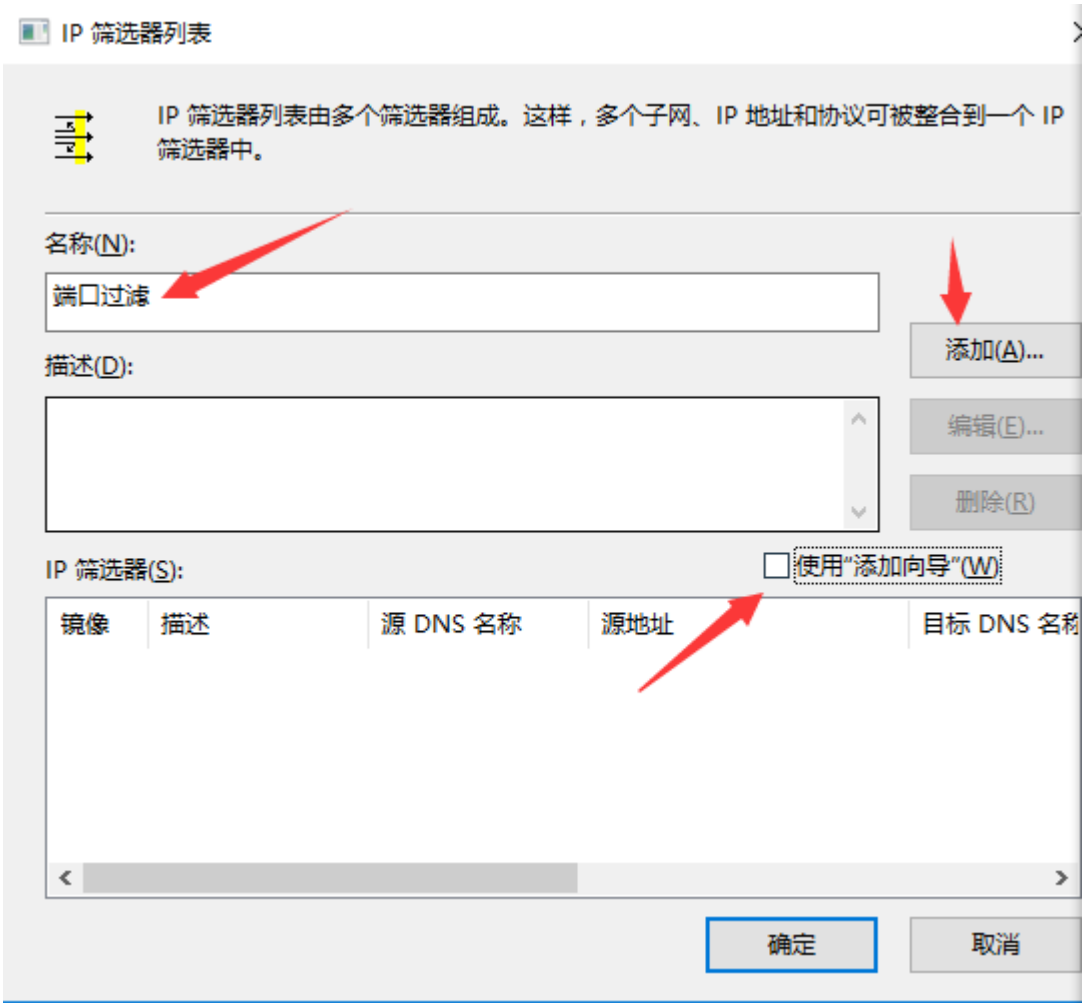
4. 去掉“使用添加向导”的勾选后，点击“添加”



5. 在新弹出的窗口，选择“IP 筛选列表”选项卡，点击“添加”

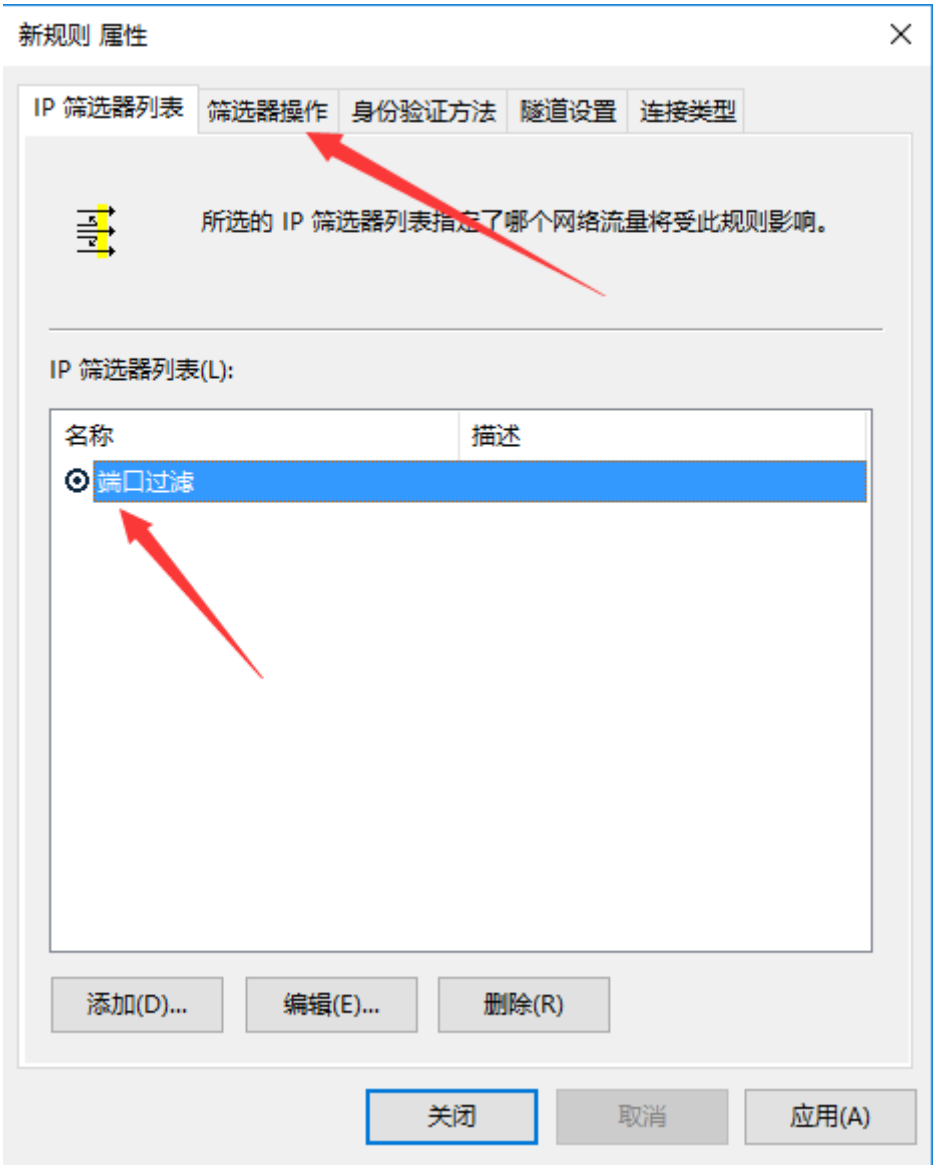


6. 在新弹出的窗口中填写名称，去掉“使用添加向导”前面的勾，单击“添加”

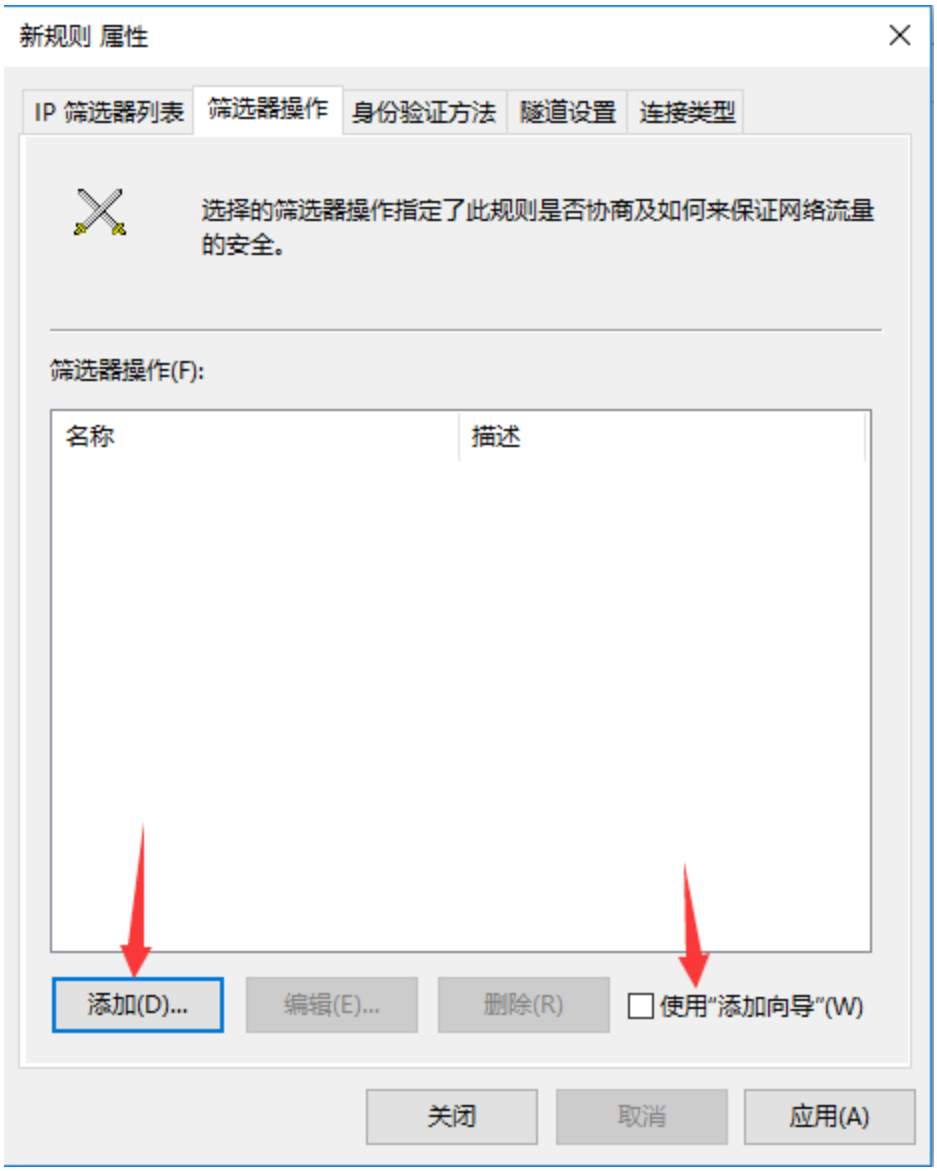


7. 在新弹出的窗口中，“协议”选项卡下，选择协议和设置到达端口信息，并点确定。

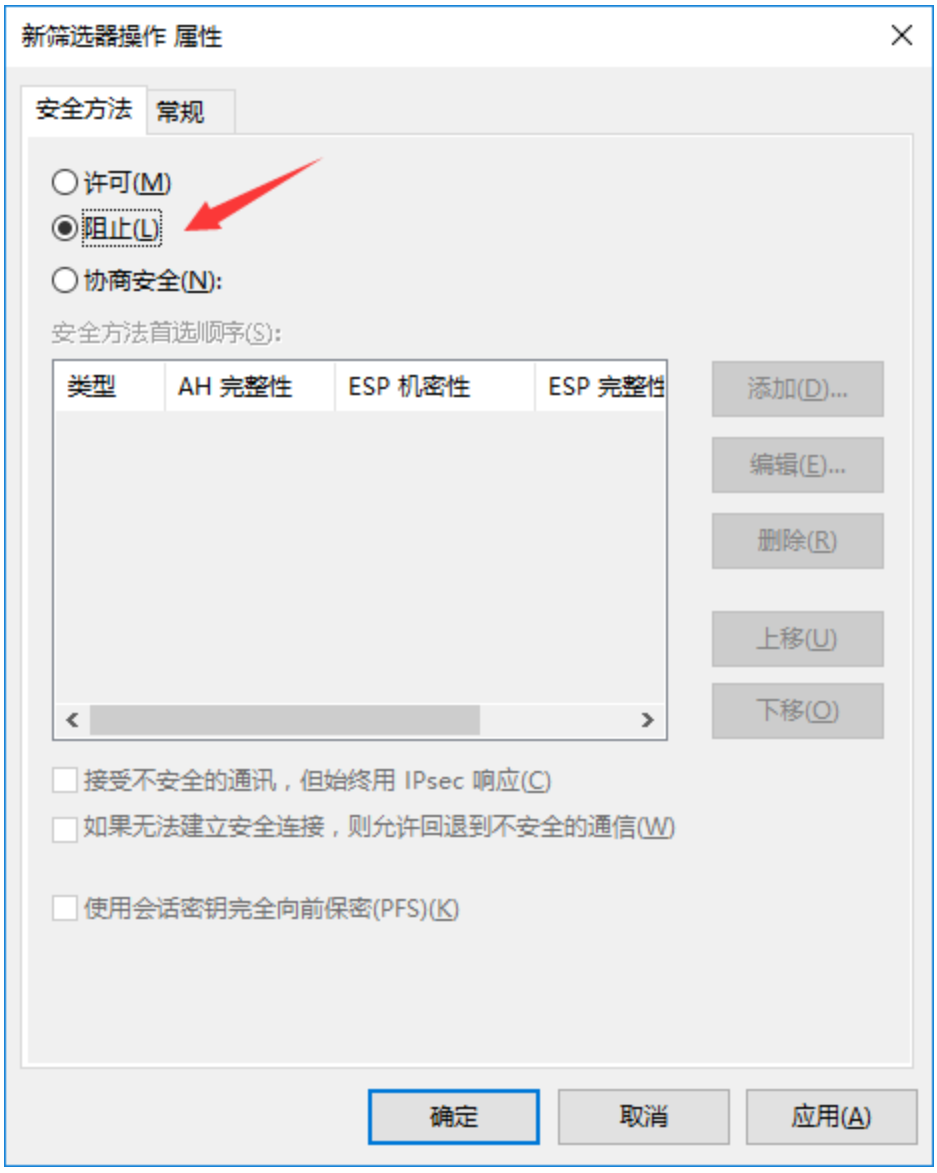
8. 重复第 7 个步骤，添加 TCP 端口 135、139、445。添加 UDP 端口 137、138。添加全部完成后，确定。
9. 选中刚添加完成的“端口过滤”规则，然后选择“筛选器操作”选项卡。



10. 去掉“使用添加向导”勾选，单击“添加”按钮

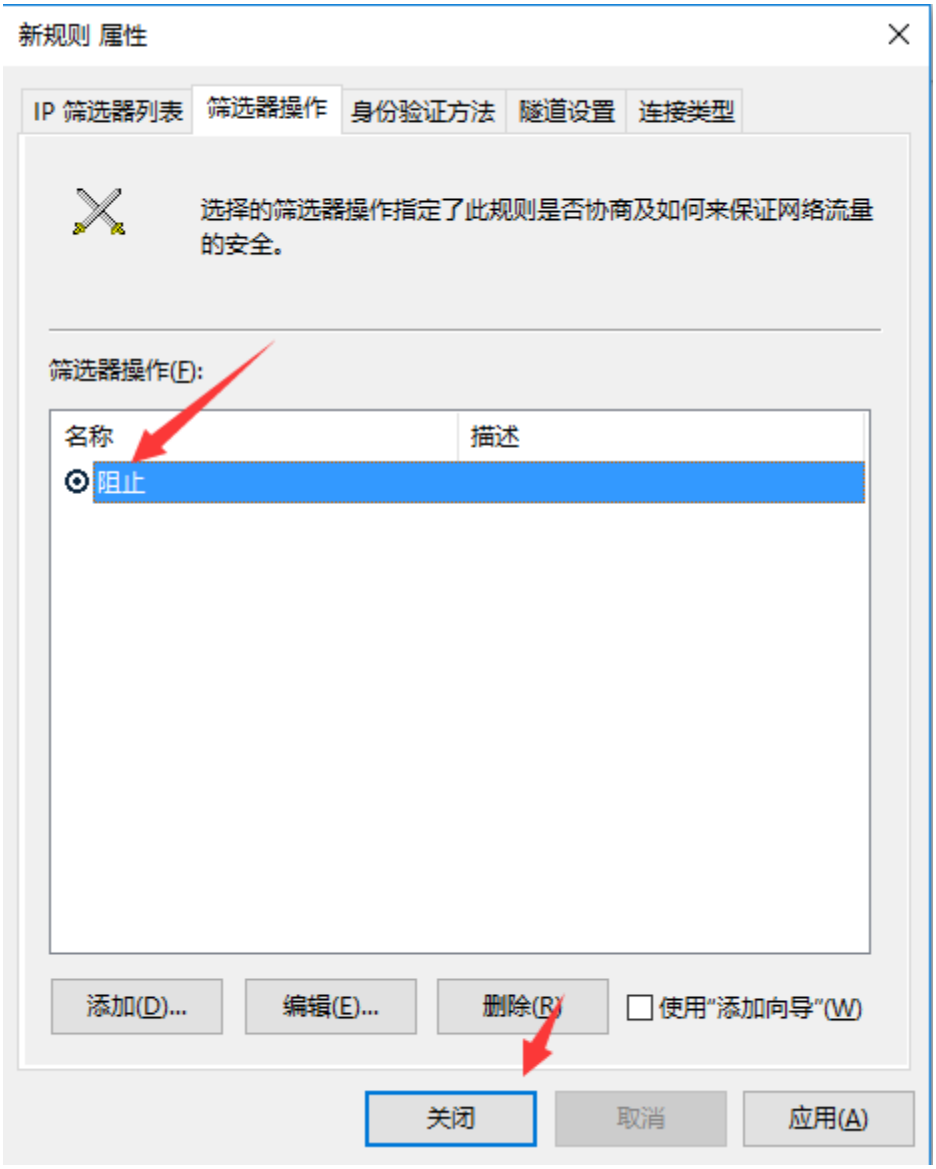

新规则 属性
IP 筛选器列表
筛选器操作
身份验证方法
隧道设置
连接类型
选择的筛选器操作指定了此规则是否协商及如何来保证网络流量的安全。
筛选器操作(F):
名称
描述
添加(D)...
编辑(E)...
删除(R)
使用“添加向导”(W)
关闭
取消
应用(A)

11. 选择“阻止”

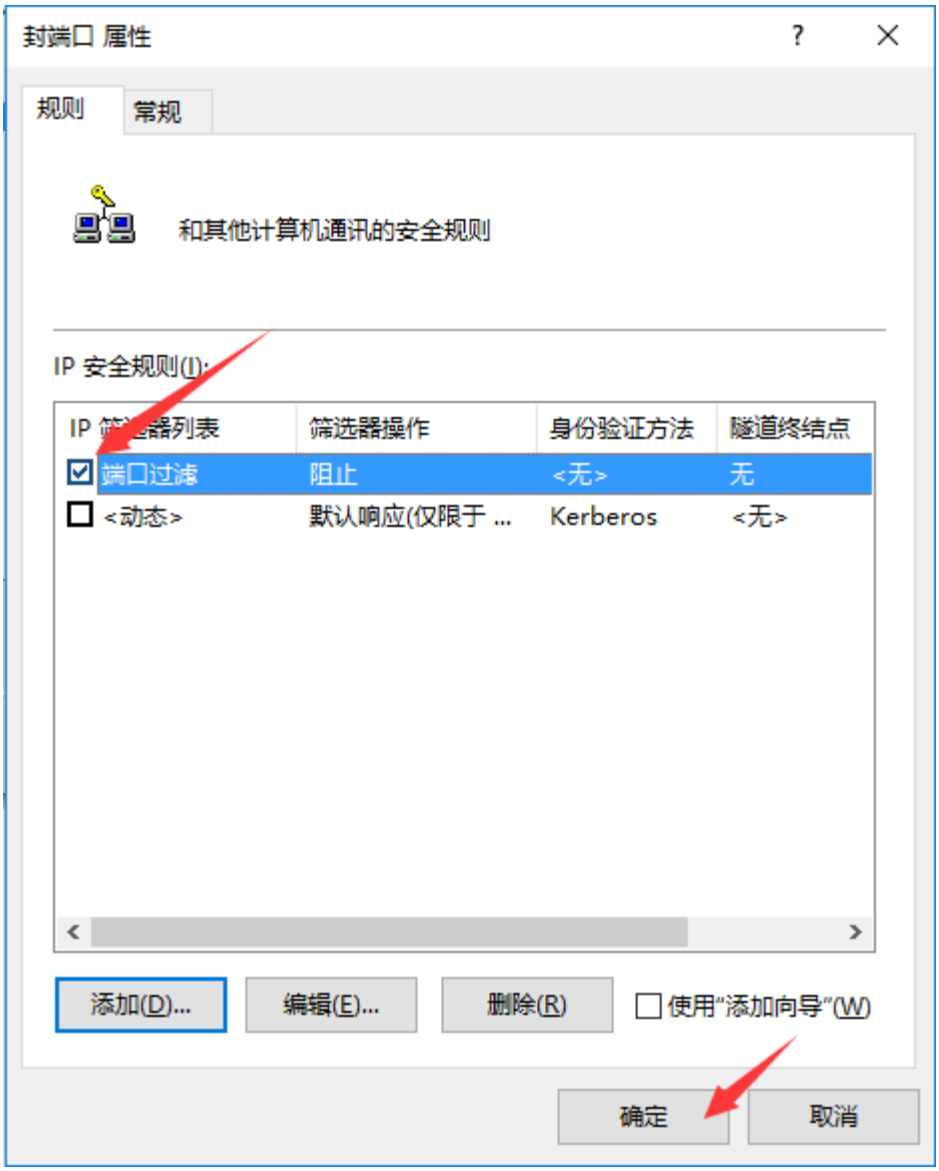


12. 选择“常规”选项卡，给这个筛选器起名“阻止”，然后“确定”。点击

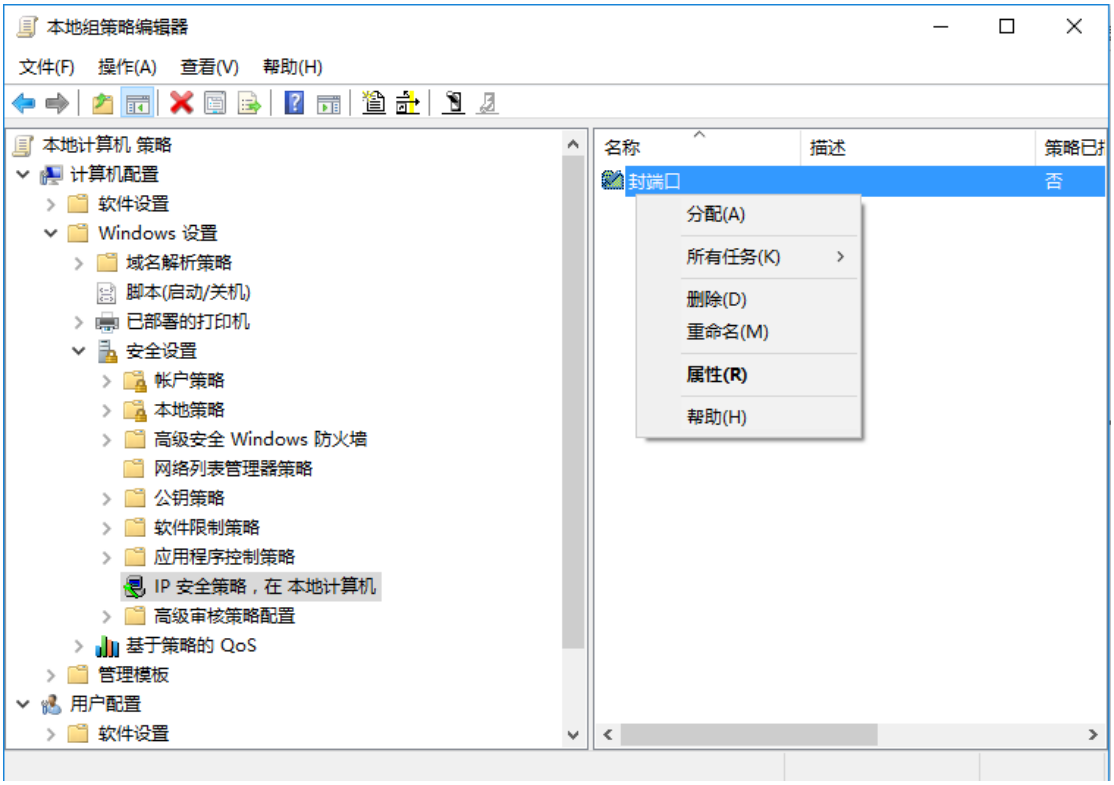
13. 确认“IP 筛选列表”选项卡下的“端口过滤”被选中。确认“筛选器操作”选项卡下的“阻止”被选中。然后点击“关闭”。



14. 确认安全规则配置正确。点击确定。



15. 在“组策略编辑器”上，右键“分配”，将规则启用。


本地组策略编辑器
文件(F)
操作(A)
查看(V)
帮助(H)
本地计算机 策略
计算机配置
软件设置
Windows 设置
域名解析策略
脚本(启动/关机)
已部署的打印机
安全设置
帐户策略
本地策略
高级安全 Windows 防火墙
网络列表管理器策略
公钥策略
软件限制策略
应用程序控制策略
IP 安全策略，在 本地计算机
高级审核策略配置
基于策略的 QoS
管理模板
用户配置
软件设置
名称
描述
封端口
否
分配(A)
所有任务(K)
删除(D)
重命名(M)
属性(R)
帮助(H)

4. 附录 – 查看 445 端口是否开放

1. 查看 445 端口是否关闭的方法：
2. 打开开始菜单---点击运行----输入 cmd---点击确定
3. 输入命令：netstat -an 回车
4. 查看结果中是否还有 445 端口