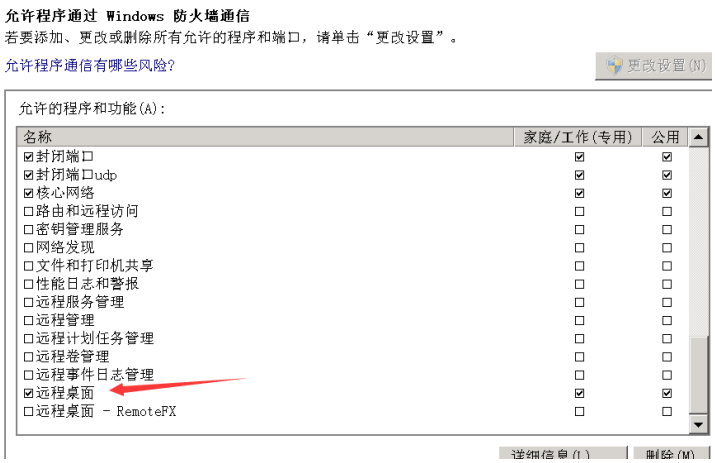
开启防火墙后如何保证远程桌面连接不中断

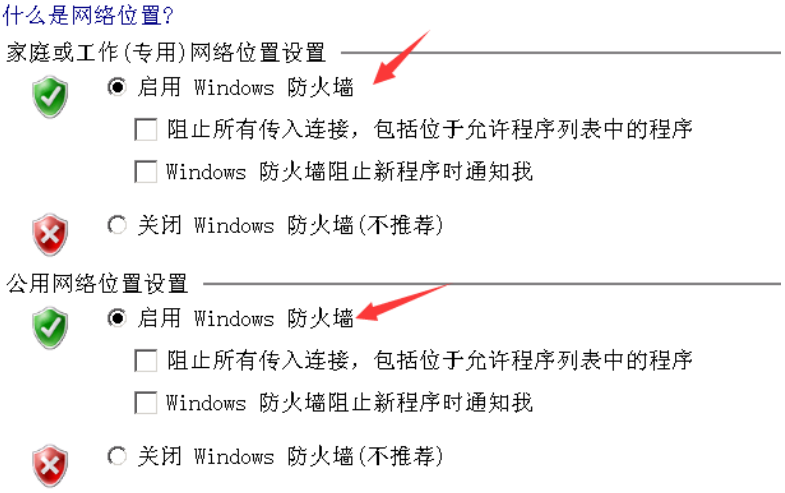
a. 在开启防火墙前，打开控制面板，点击检查防火墙状态

b. 点击允许程序或功能通过 Windows 防火墙

c. 勾选远程桌面，然后点击确定即可。



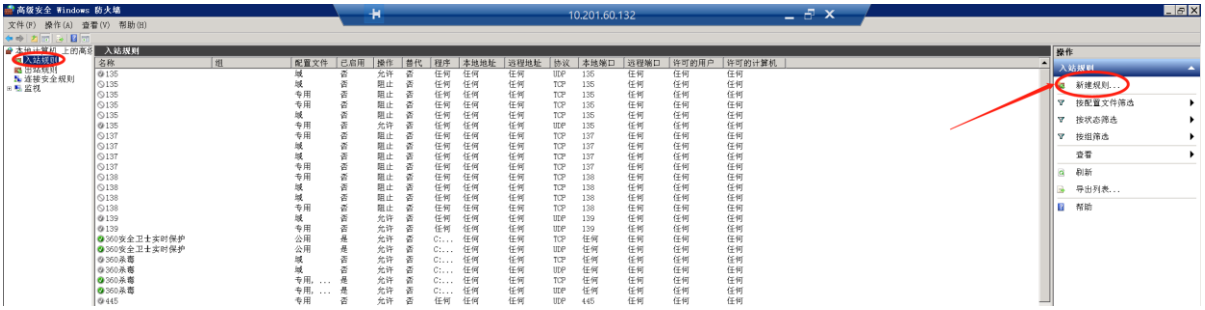
d. 点击打开或关闭 windows 防火墙，点击启用 windows 防火墙。



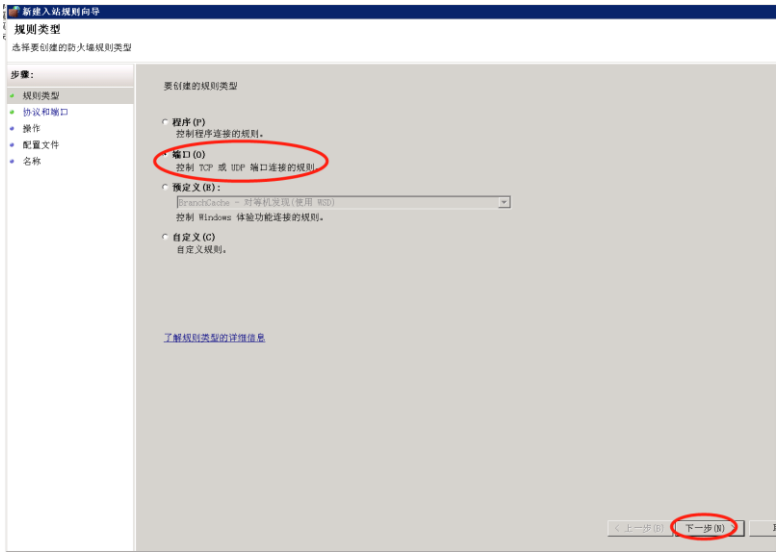
开启防火墙后如何保证原有应用的访问正常

a.打开 windows 防火墙，然后点击高级设置

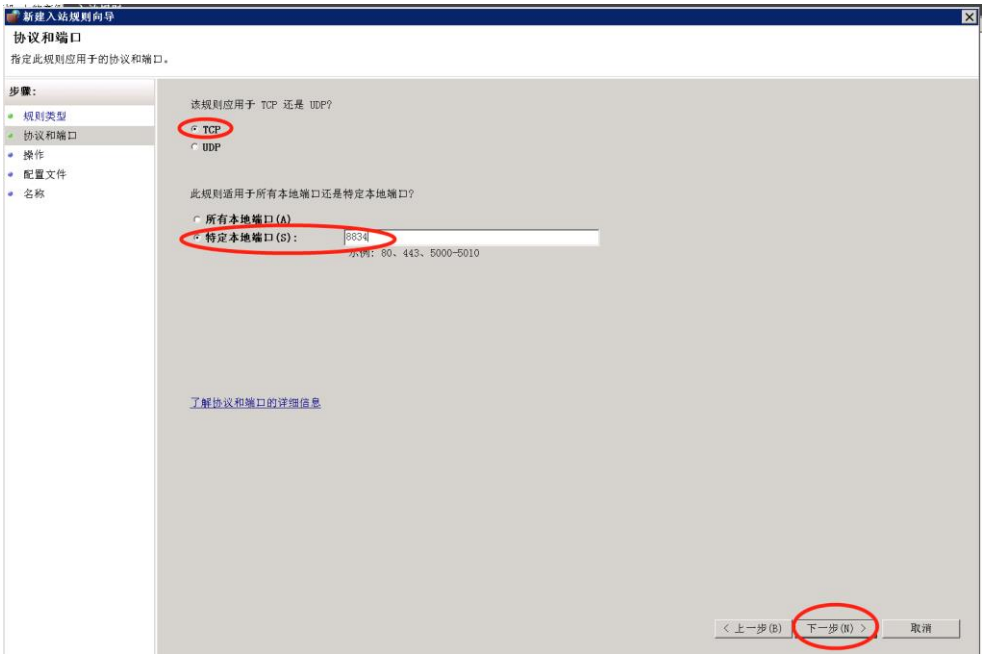
b.点击入站规则，然后点击新建规则



c.点击端口，下一步。



d.选择 tcp，然后输入需要越过防火墙的端口，以 web 端口 8834 做例，点击下一步。



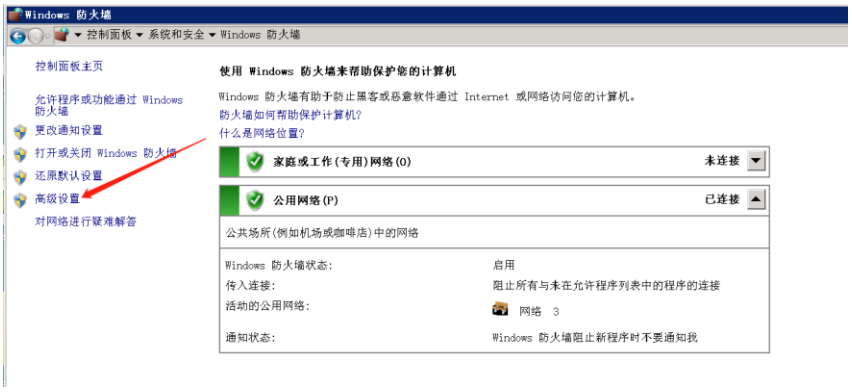
e.选择允许连接，下一步。

f.域，专用，公用全勾，下一步。

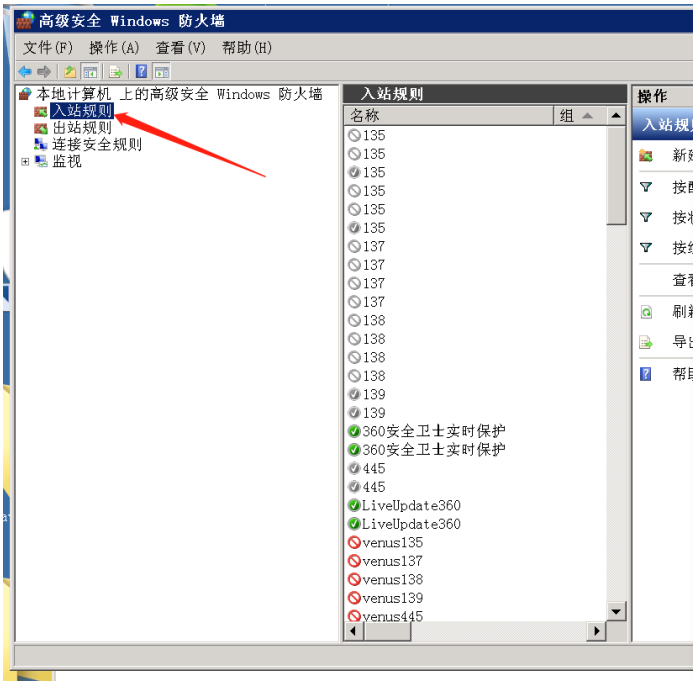
g.给策略取个名称，完成。

如何关闭高危端口

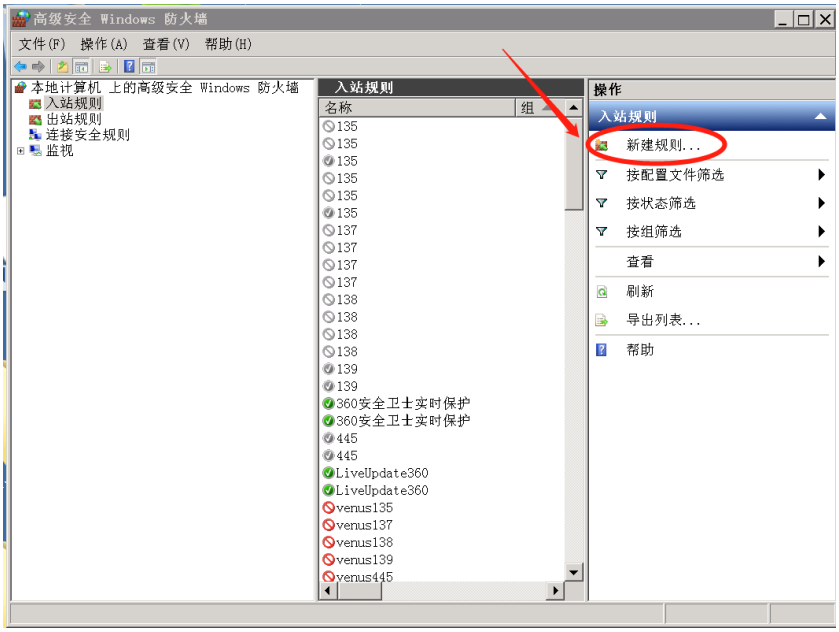
a. 如图所示，打开电脑的控制面板，选择系统和安全，进入 windows 防火墙，在放火墙页面左侧的选项卡中选择高级设置。



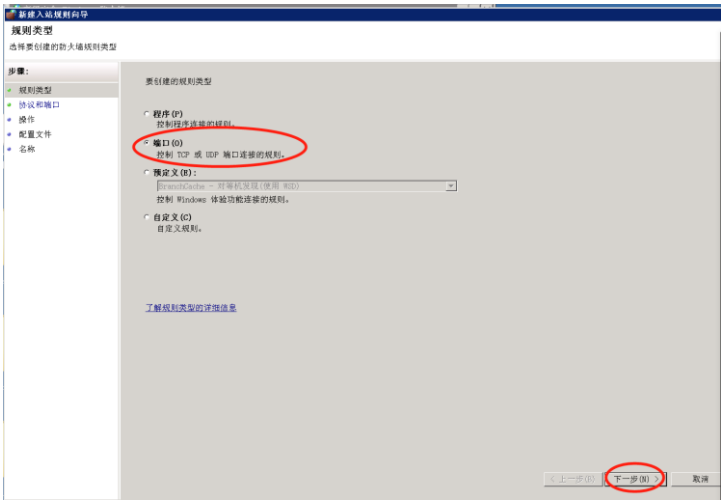
b.进入高级设置页面，在页面左侧的选项卡中选择入站规则，点击进入。



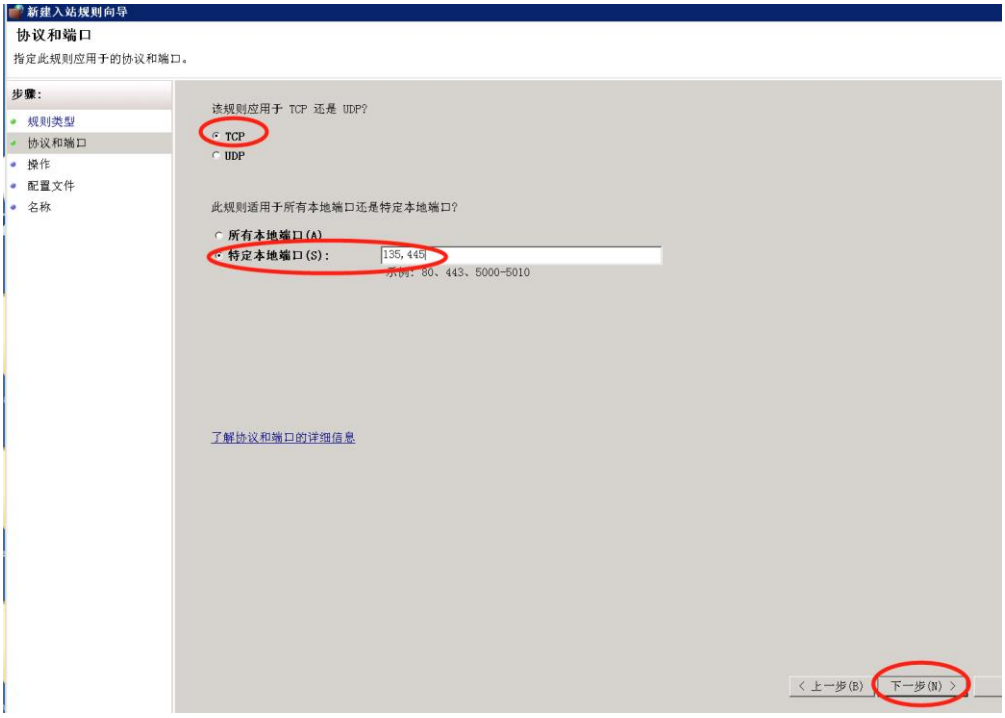
c.进入入站规则页面后，选择页面右侧选项中的新建规则，图中红色圆圈位置。



d.在弹出的新建入站规则向导页面中，在“要创建的规则类型”选项中选择“端口”项，然后点击下一步进入下一个页面。

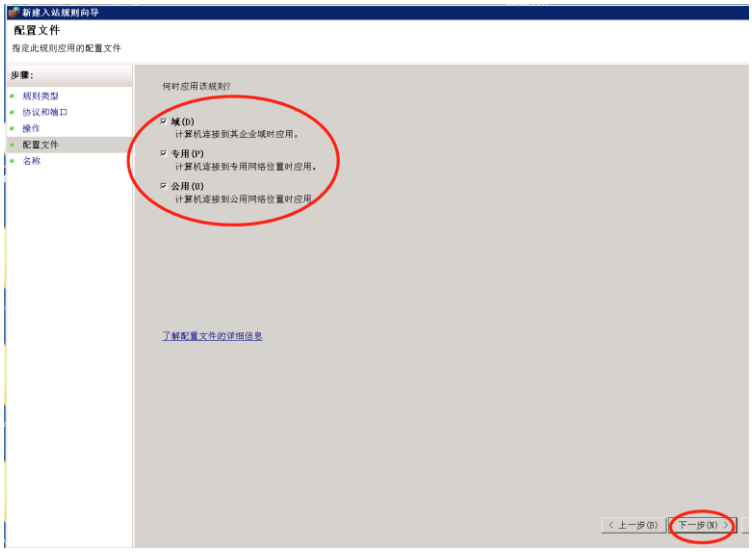


e. 在新页面选项中选择“特定的本地端口”,输入想要禁止的端口，以 135 和 445 两端口为例，在框中输入 135,445，中间用逗号隔开。至于 TCP 和 UDP，两个协议都需要封闭，但不能同时进行，先选择 TCP 协议。设置完成后点击“下一步”。

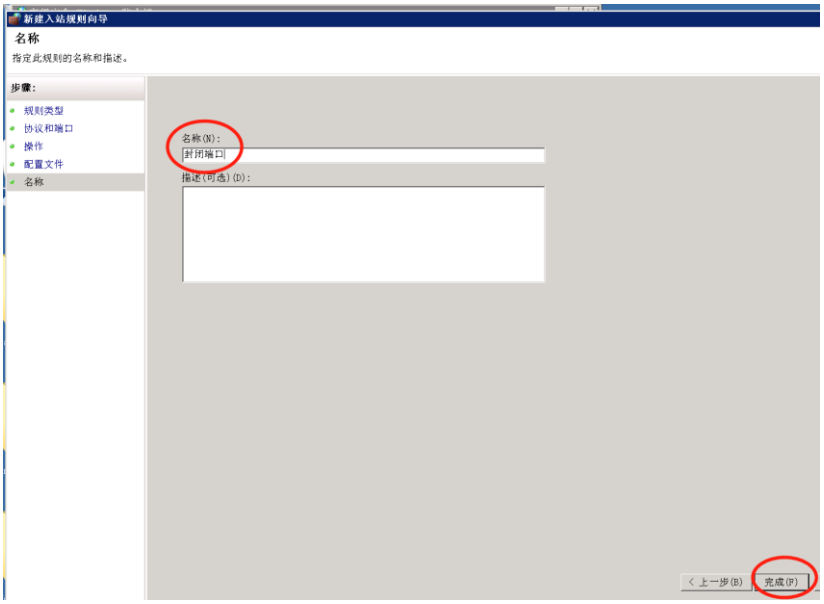


f. 在接下来的页面中选择“阻止连接”项，点击下一步。

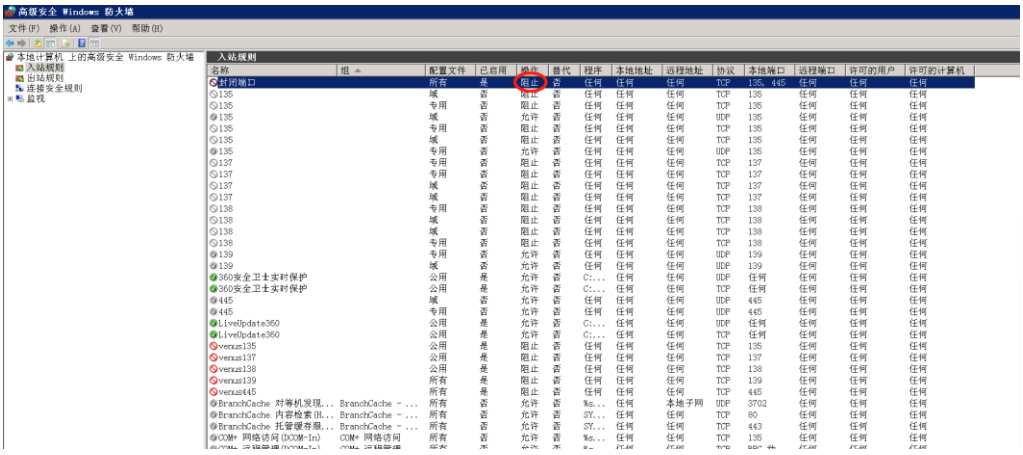
g. 在“何时应用该规则”选项中全选，进入下一步。



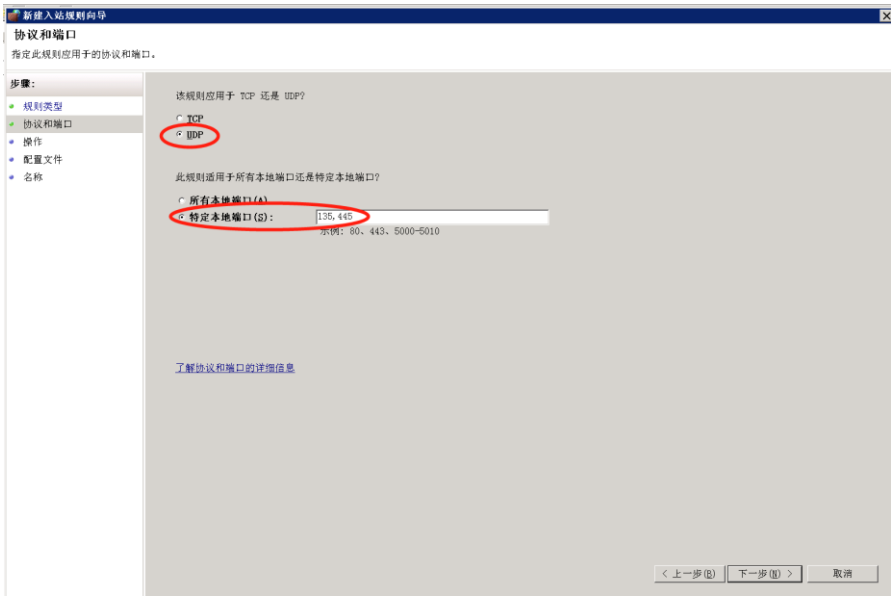
h. 在接下来的页面中名称输入栏内，输入任何名称，点击完成。



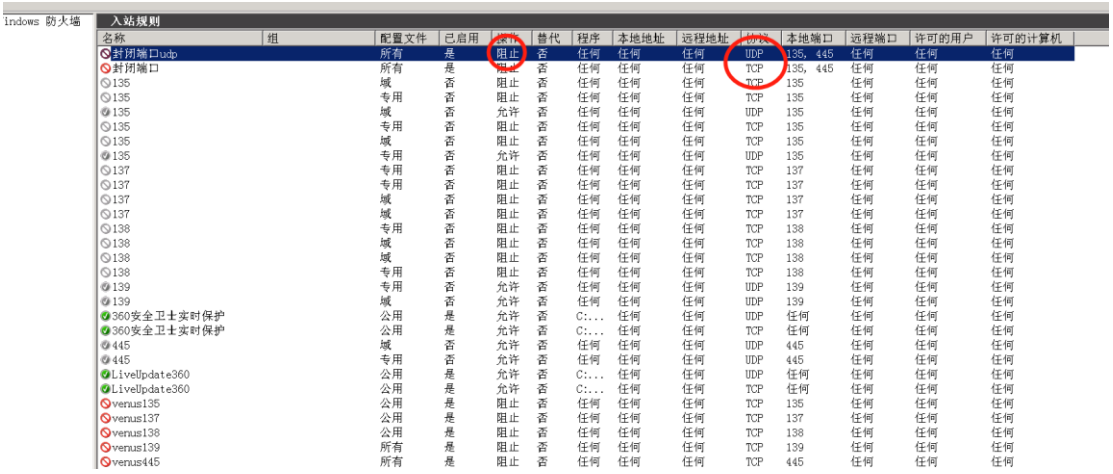
i. 至此，该操作已完成，我们可以在入站规则页面看到 TCP 协议中 135 和 445 端口已被阻止使用。



j. 按照上述步骤，再次进入新建规则，在封闭端口选项中选择 UDP 协议进行端口封闭操作，步骤与 TCP 协议端口封闭完全相同。



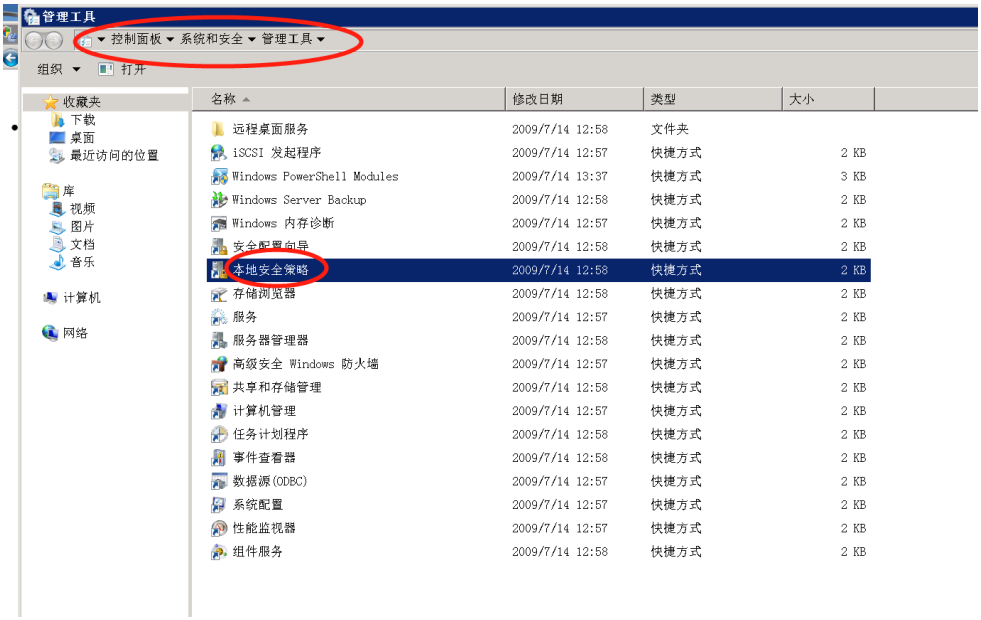
k. 依次完成阻止连接、随意输入名称操作后，进入入站规则页面，向右滚动滑条，可以看到 135 和 445 端口均已被阻止连接。



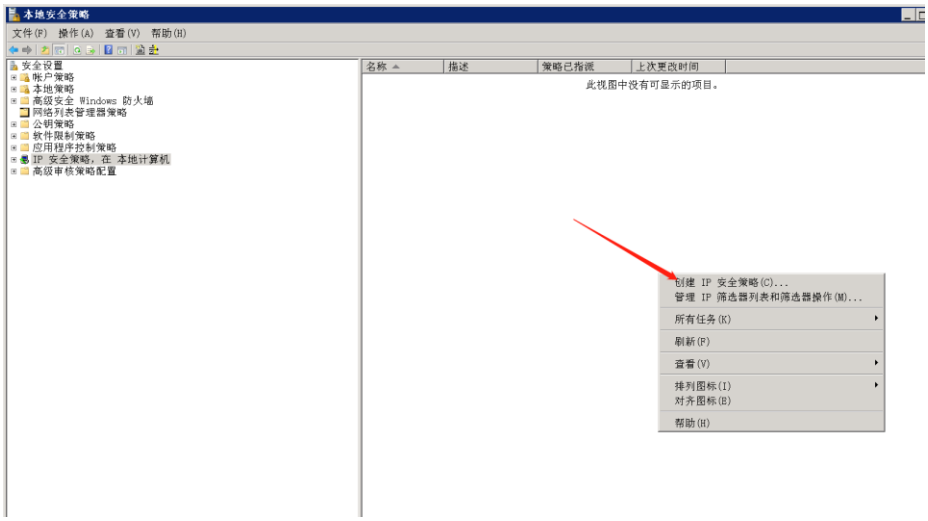
名称	组	配置文件	已启用	操作	替代	程序	本地地址	远程地址	协议	本地端口	远程端口	许可的用户	许可的计算机
封闭端口udp		所有	是	阻止	否	任何	任何	任何	UDP	135, 445	任何	任何	任何
封闭端口		所有	是	阻止	否	任何	任何	任何	TCP	135, 445	任何	任何	任何
135		域	否	阻止	否	任何	任何	任何	TCP	135	任何	任何	任何
135		专用	否	阻止	否	任何	任何	任何	TCP	135	任何	任何	任何
135		域	否	允许	否	任何	任何	任何	UDP	135	任何	任何	任何
135		专用	否	阻止	否	任何	任何	任何	TCP	135	任何	任何	任何
135		域	否	阻止	否	任何	任何	任何	TCP	135	任何	任何	任何
135		专用	否	允许	否	任何	任何	任何	UDP	135	任何	任何	任何
137		专用	否	阻止	否	任何	任何	任何	TCP	137	任何	任何	任何
137		专用	否	阻止	否	任何	任何	任何	TCP	137	任何	任何	任何
137		域	否	阻止	否	任何	任何	任何	TCP	137	任何	任何	任何
137		域	否	阻止	否	任何	任何	任何	TCP	137	任何	任何	任何
138		专用	否	阻止	否	任何	任何	任何	TCP	138	任何	任何	任何
138		域	否	阻止	否	任何	任何	任何	TCP	138	任何	任何	任何
138		域	否	阻止	否	任何	任何	任何	TCP	138	任何	任何	任何
138		专用	否	阻止	否	任何	任何	任何	TCP	138	任何	任何	任何
139		专用	否	允许	否	任何	任何	任何	UDP	139	任何	任何	任何
139		域	否	允许	否	任何	任何	任何	UDP	139	任何	任何	任何
360安全卫士实时保护		公用	是	允许	否	C:...	任何	任何	UDP	任何	任何	任何	任何
360安全卫士实时保护		公用	是	允许	否	C:...	任何	任何	TCP	任何	任何	任何	任何
445		域	否	允许	否	任何	任何	任何	UDP	445	任何	任何	任何
445		专用	否	允许	否	任何	任何	任何	UDP	445	任何	任何	任何
LiveUpdate360		公用	是	允许	否	C:...	任何	任何	UDP	任何	任何	任何	任何
LiveUpdate360		公用	是	允许	否	C:...	任何	任何	TCP	任何	任何	任何	任何
venus135		公用	是	阻止	否	任何	任何	任何	TCP	135	任何	任何	任何
venus137		公用	是	阻止	否	任何	任何	任何	TCP	137	任何	任何	任何
venus138		公用	是	阻止	否	任何	任何	任何	TCP	138	任何	任何	任何
venus139		所有	是	阻止	否	任何	任何	任何	TCP	139	任何	任何	任何
venus445		所有	是	阻止	否	任何	任何	任何	TCP	445	任何	任何	任何

如何限制只有部分 IP 才能访问高危端口

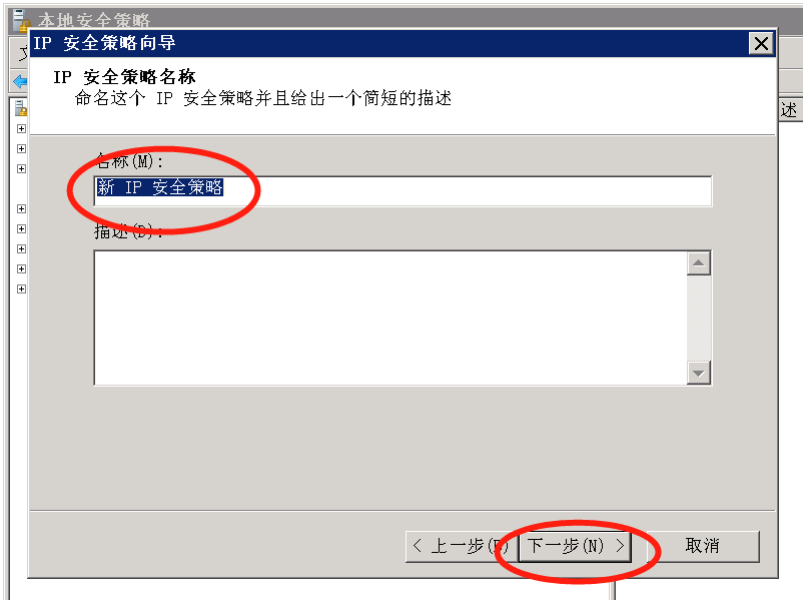
a.打开控制面板，系统和安全，选择管理工具，接着选择本地安全策略



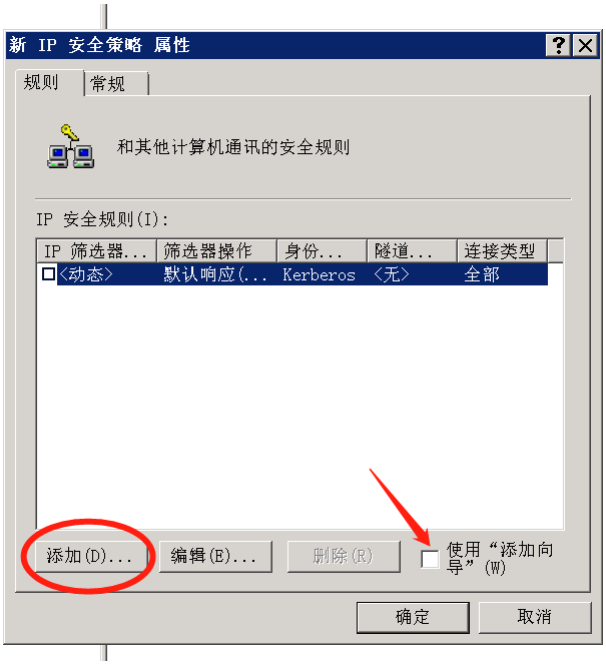
b.打开本地安全策略后选择左边的“IP 安全策略，在本地计算机”，在右边空白处右键单击，选择创建 IP 安全策略。



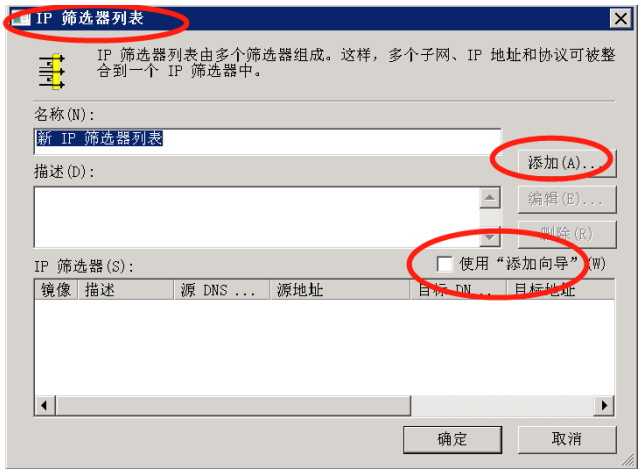
c.向导弹出后根据需要填写一下策略名称和描述，单击下一步直到结束，选择完成



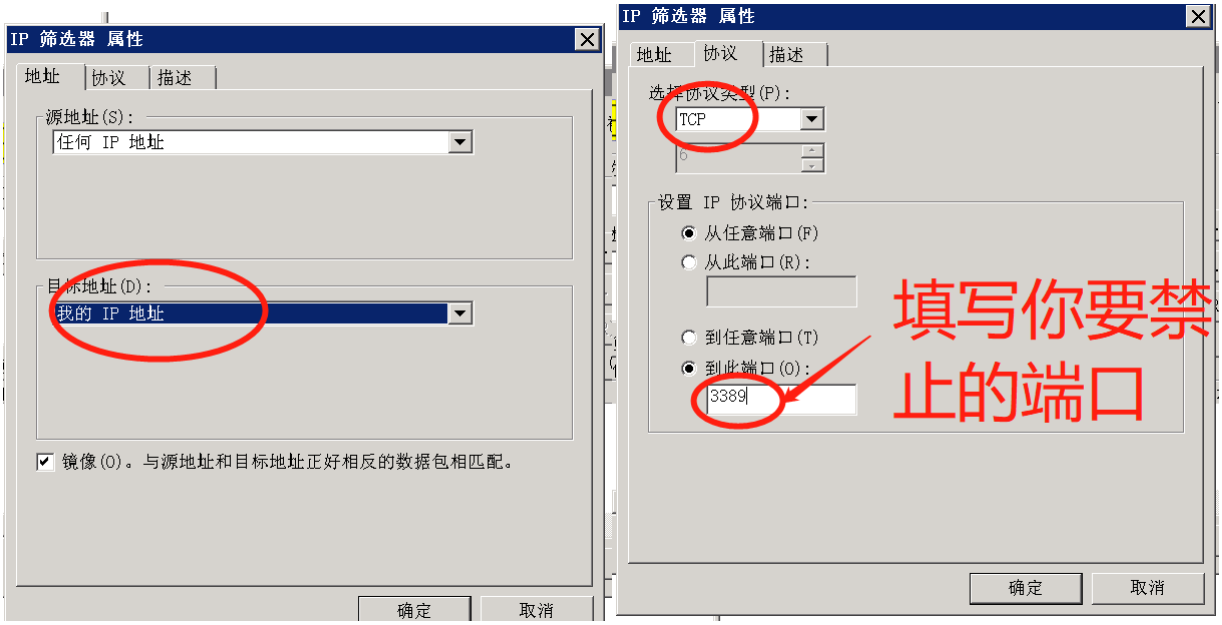
d.在随后弹出的界面中取消勾选“使用向导”，再单击添加



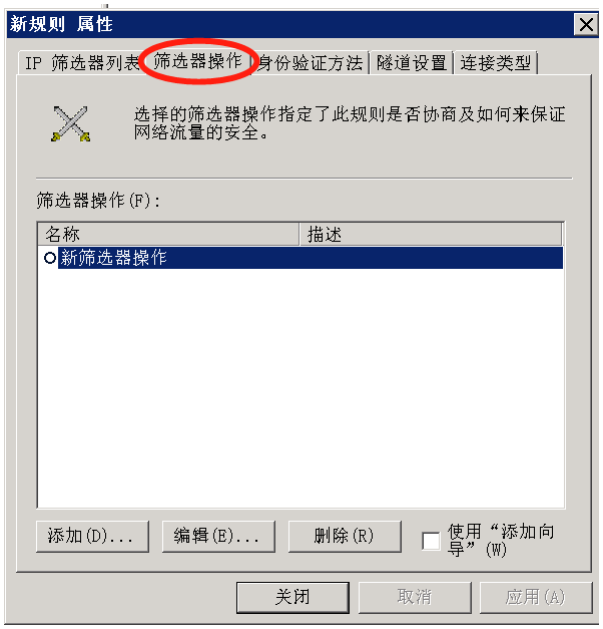
e.接下来的页面中切换到 IP 筛选器列表单击添加，接着取消勾选使用“添加向导”，然后单击添加



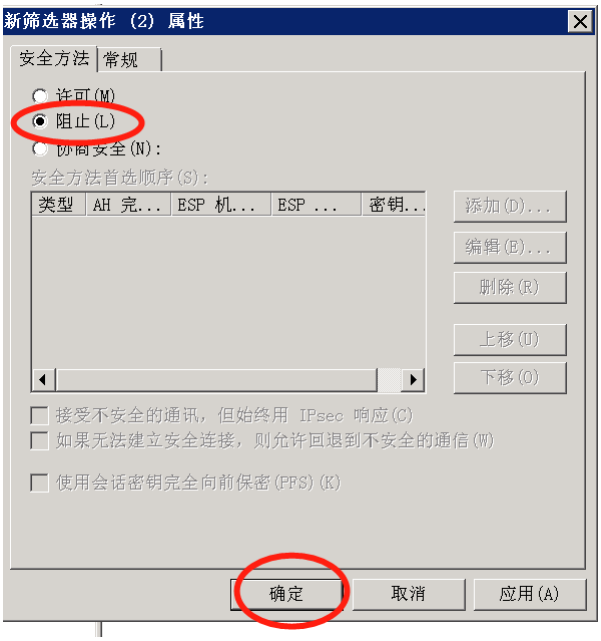
f.在弹出的向导内按下图设置。



g.接下来确定，回到最初界面，选中新建的筛选器规则后切换到筛选器操作



h.依然取消勾选使用向导，单击添加，选择阻止，单击确定



i.接着选中新筛选器操作，单击确定回到起始界面

j.最后在新建的策略上右键单击，选择分配最后重启计算机即可