由于近日爆发WannaCry勒索病毒，此病毒可在局域网内通过445端口自行传播，为了避免周一上班后刚开机就被感染，且把硬盘所有文件都加密，请开机前先断网，按顺序执行如下6条防护操作，windows服务器运维人员请尽早执行。

已经发现自己中病毒，文件被加密的电脑、服务器，禁止接入网络！

防护操作：

1 断网（拔网线）

2 开机（若关机状态）

3 关闭445端口

**(1) Win7、Win8、Win10的处理流程**

1、打开控制面板-系统与安全-Windows防火墙，点击左侧启动或关闭Windows防火墙



2、选择启动防火墙，并点击确定



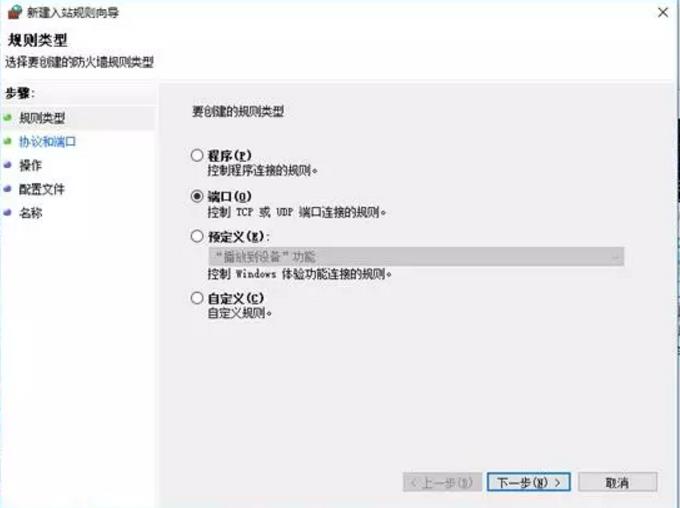
3、点击高级设置



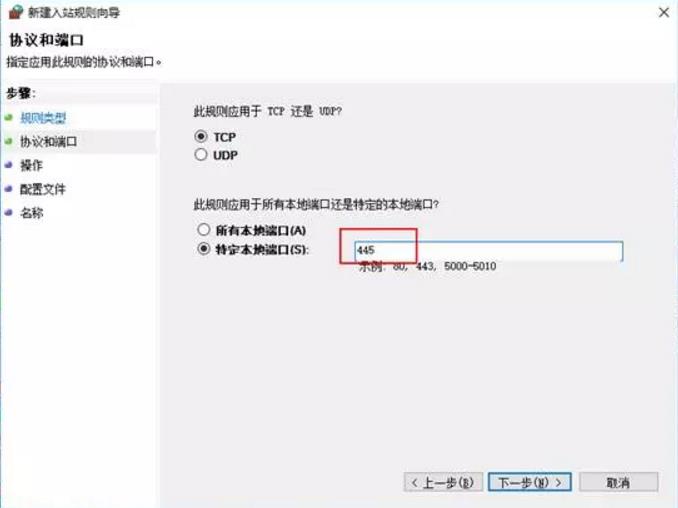
4、点击入站规则，新建规则



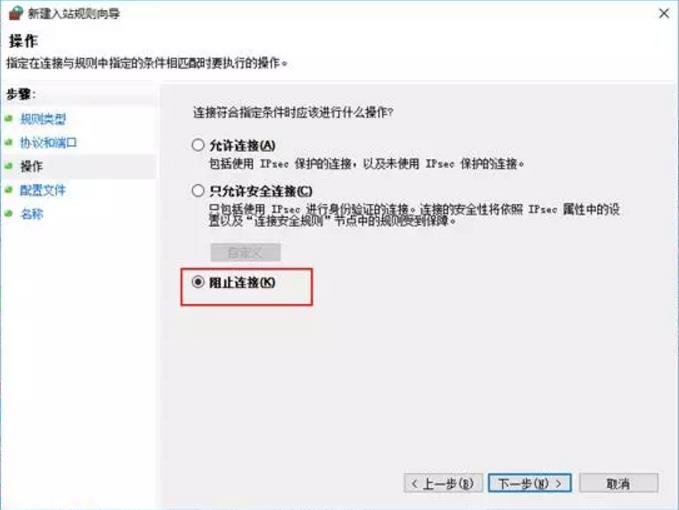
5、选择端口，下一步



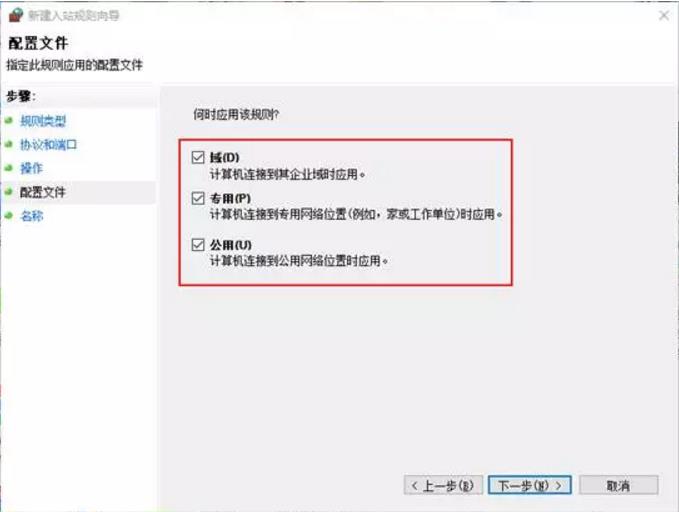
6、特定本地端口，输入445，下一步



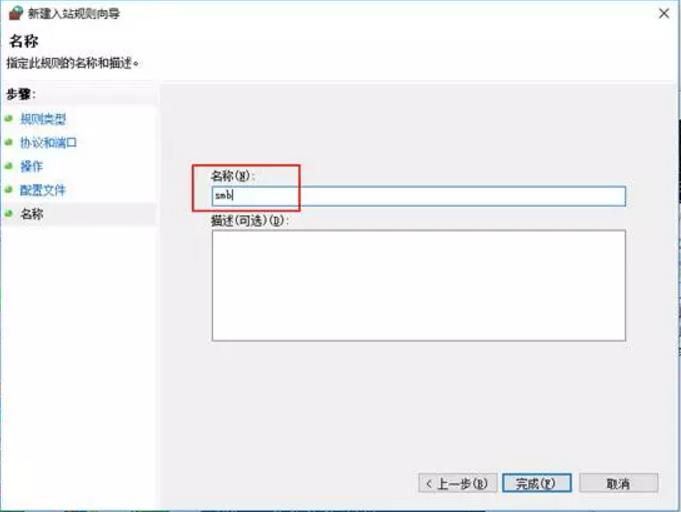
7、选择阻止连接，下一步



8、配置文件，全选，下一步

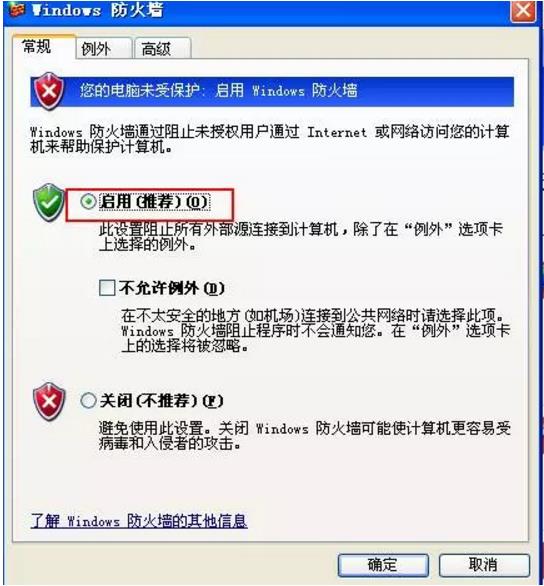


9、名称，可以任意输入，完成即可。

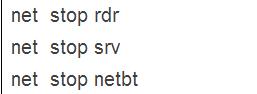


**(2)  XP系统的处理流程**

1、依次打开控制面板，安全中心，Windows防火墙，选择启用



2、点击开始，运行，输入cmd，确定执行下面三条命令



4 确认445端口关闭

本机cmd窗口执行命令"netstat -ano | findstr ":445""，回车后无任何返回。

5使用U盘或者各类网盘将你的重要资料进行备份；

6联网打补丁

微软之前已经停止更新的操作系统（如XP,2003），可以在如下链接找到这个漏洞的补丁：<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>。