重要通知：勒索病毒防治指南

学校正版软件管理平台（software.bnu.edu.cn）向所有师生提供免费的各版本操作系统，同时提供补丁客户端（校内免流量），强烈建议大家使用学校提供的正版软件并打开自动更新和防火墙。

WannaCry勒索病毒今天已出现变种，未修复该漏洞的用户请尽快处理。此病毒通过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4条防护操作。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（见后面方法）

4 联网打补丁（使用学校提供的正版操作系统可去正版软件管理平台下载补丁客户端software.bnu.edu.cn）

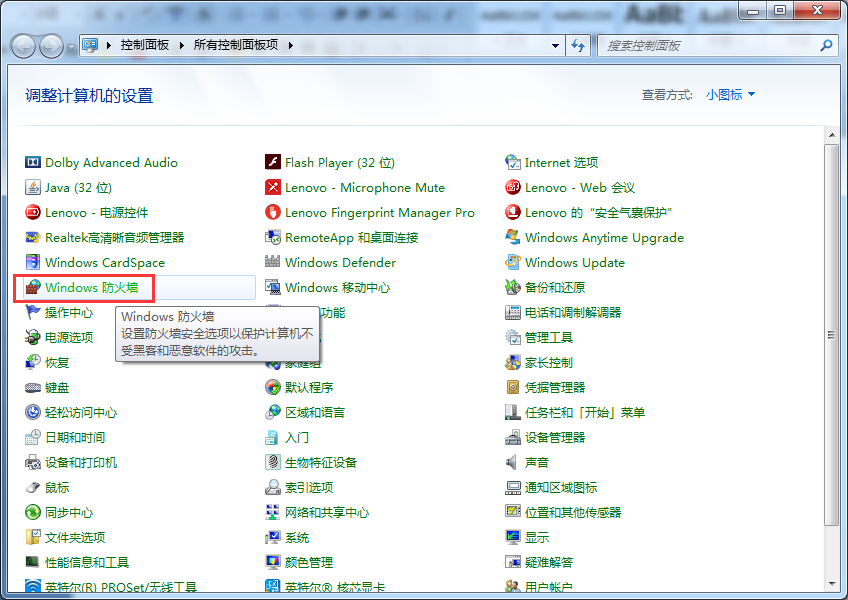
非使用学校正版操作系统Win7及以上版本微软官方补丁下载：

https://technet.microsoft.com/zh-cn/library/security/MS17-010.aspx

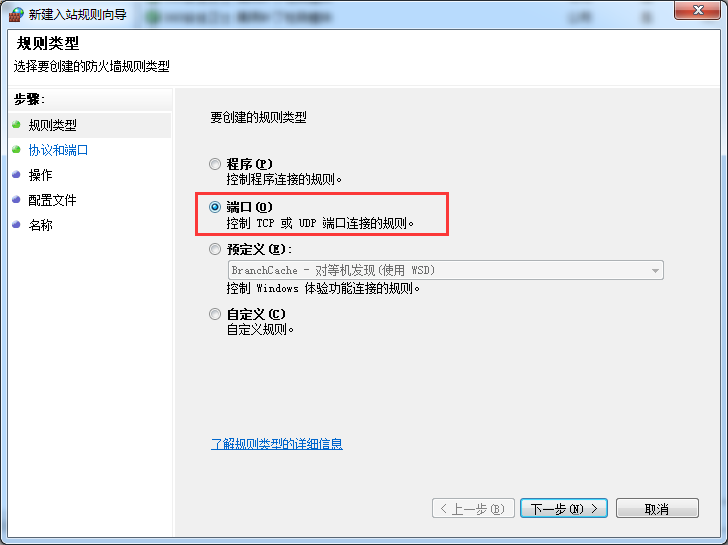
微软之前已经停止更新的操作系统（如XP,2003），可以在如下链接找到这个漏洞的补丁：<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>

关445端口方法：按图配置防火墙

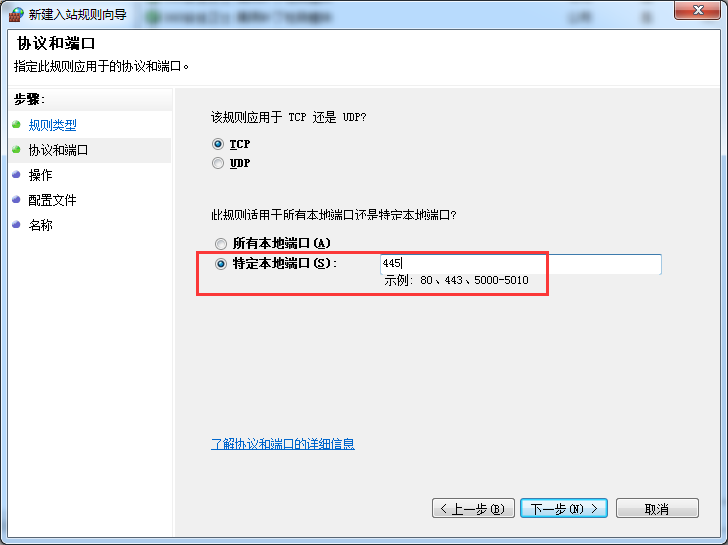
1. 控制面板->windows防火墙



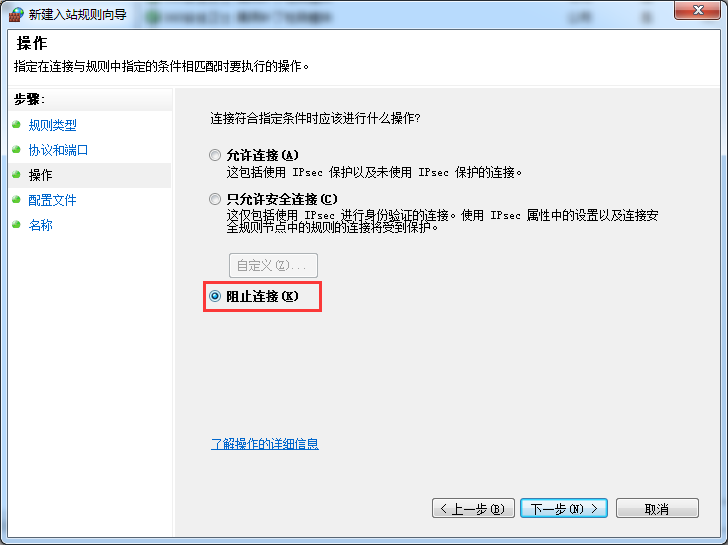
1. 高级设置->入站规则(右键)->新建规则
2. 选择“端口”->下一步



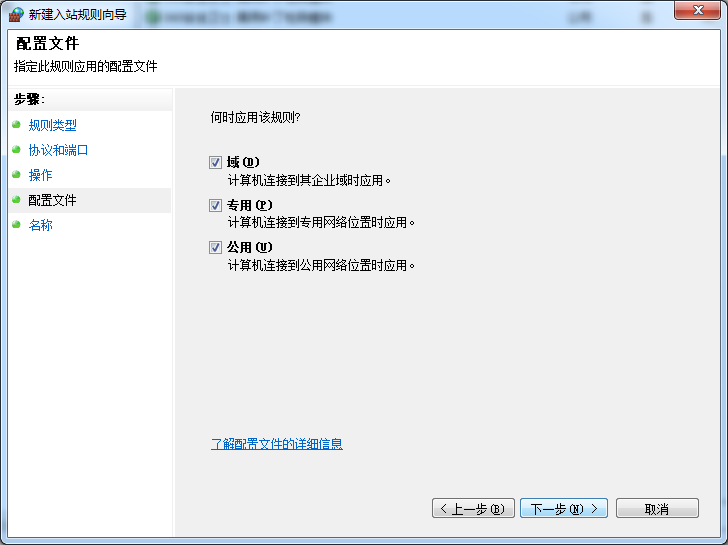
1. 选择tcp，指定对应端口（以445端口为例）



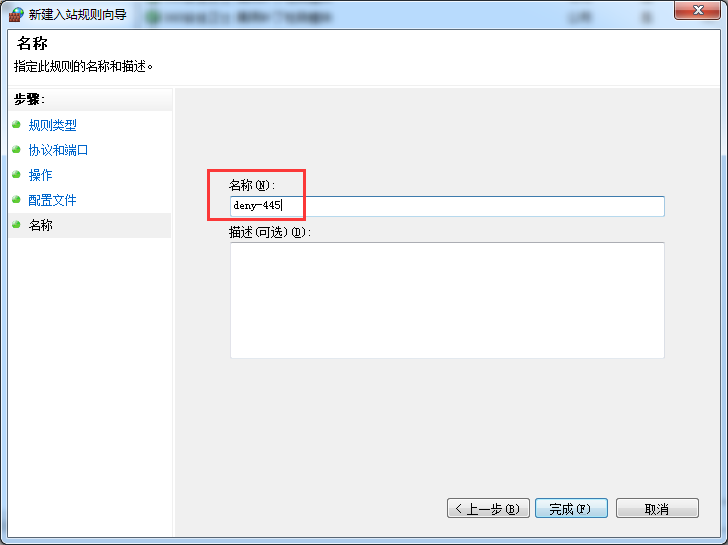
1. 选择“阻止连接”->下一步



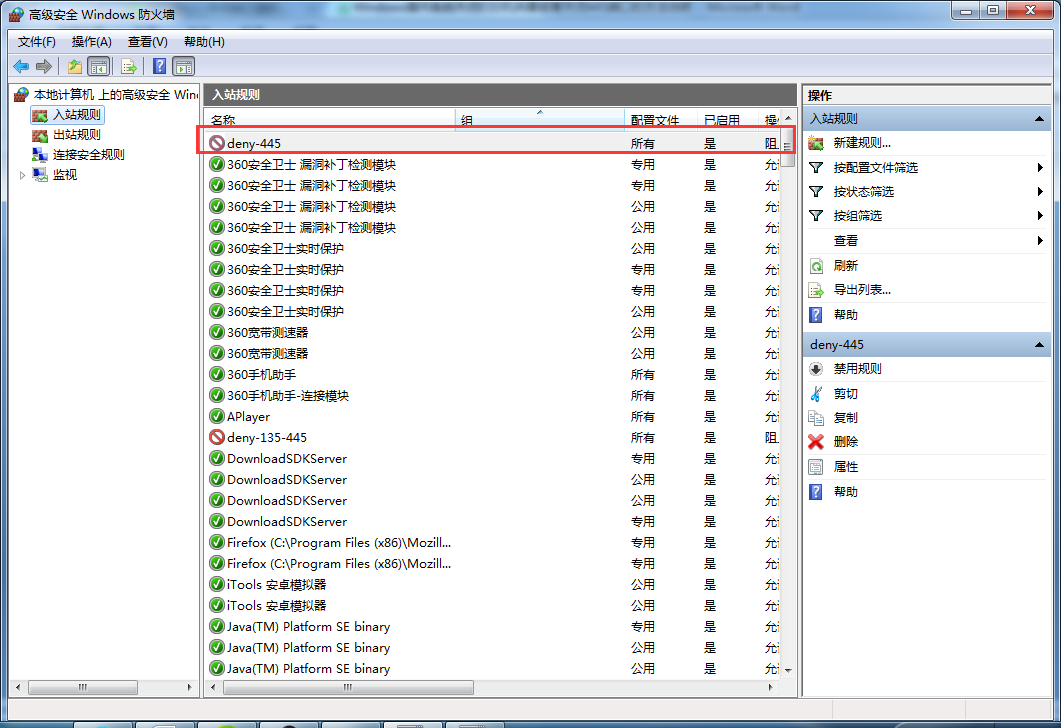
1. 全选->下一步



1. 为这条新建规则命名,例如"deny-445"->完成



1. 然后就可以看到状态了，启用阻止445端口成功～



其它参考防护工具

360 企业安全天擎团队已经针对 WannaCry 勒索蠕虫开发了一款免疫工具，

此程序在电脑上运行以后，现有蠕虫将不会感染系统。免疫工具下载地址：

http://b.360.cn/other/onionwormimmune。

同时开发了一款勒索蠕虫漏洞修复工具，此修复工具集成免疫、SMB 服务关

闭和各系统下 MS17-010 漏洞检测与修复于一体。可在离线网络环境下一键式修

复系统存在的 MS17-010 漏洞，根本解决勒索蠕虫利用 MS17-010 漏洞带来的安全

隐患。修复工具下载地址： http://b.360.cn/other/onionwormfix。