周一上班第一件事：

拔网线，再开机打补丁

由于近日爆发 WannaCry 勒索病毒及其同系列变种，此病毒可在局域网内通过 445 端口自行传播，因大部分终端周末处于关闭状态，为了避免周一上班后大量未做安全加固的终端集中开机，导致病毒感染，重要文件被锁住。请各位员工在开机前务必先断开网络，并按以下顺序执行如下 5 条防护操作，各类 Windows 服务器运维人员请尽早执行。

另：请各位员工同时注意做好重要文件的备份工作。

如果已经发现中病毒，文件被加密的电脑、服务器等的，请立即拔出网线，断开一切有线、无线等网络连接，并立即联系技术支撑人员！

防护操作具体步骤：

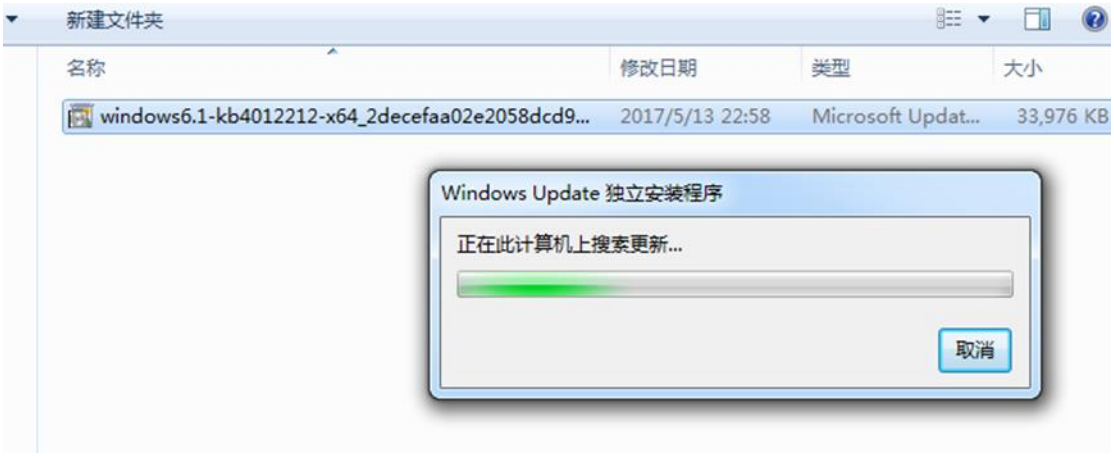
1. 断网（拔网线，关闭无线开关）
2. 开机（若关机状态）
3. 关闭 445 端口（见后面方法一或方法二）
4. 联网打补丁

1) Win7 以上系统可通过自动更新或下载公司 OA 门户提供的补丁进行安装，内部下载地址：

http://www.sh.ctc.com/portalwas1/IdealCMS/contentview.view?id=8a87cbc85bed1143015c04b708f1166b&flag=0&

完成下载后解压补丁：

进入与自己操作系统相匹配的补丁目录，64 位操作系统选择 x64 版本，32 位操作系统选择 x86 版本



运行相应补丁，更新完成后重启主机即可。

2) WinXp 和 Win2003 系统打补丁参见方法二。

附：Windows 系统加固方法步骤：

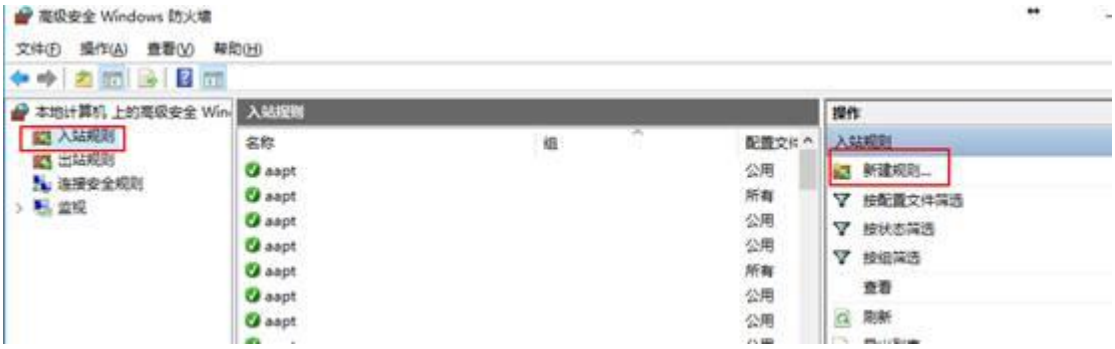
方法一、Win7、Win8、Win10 的处理流程

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

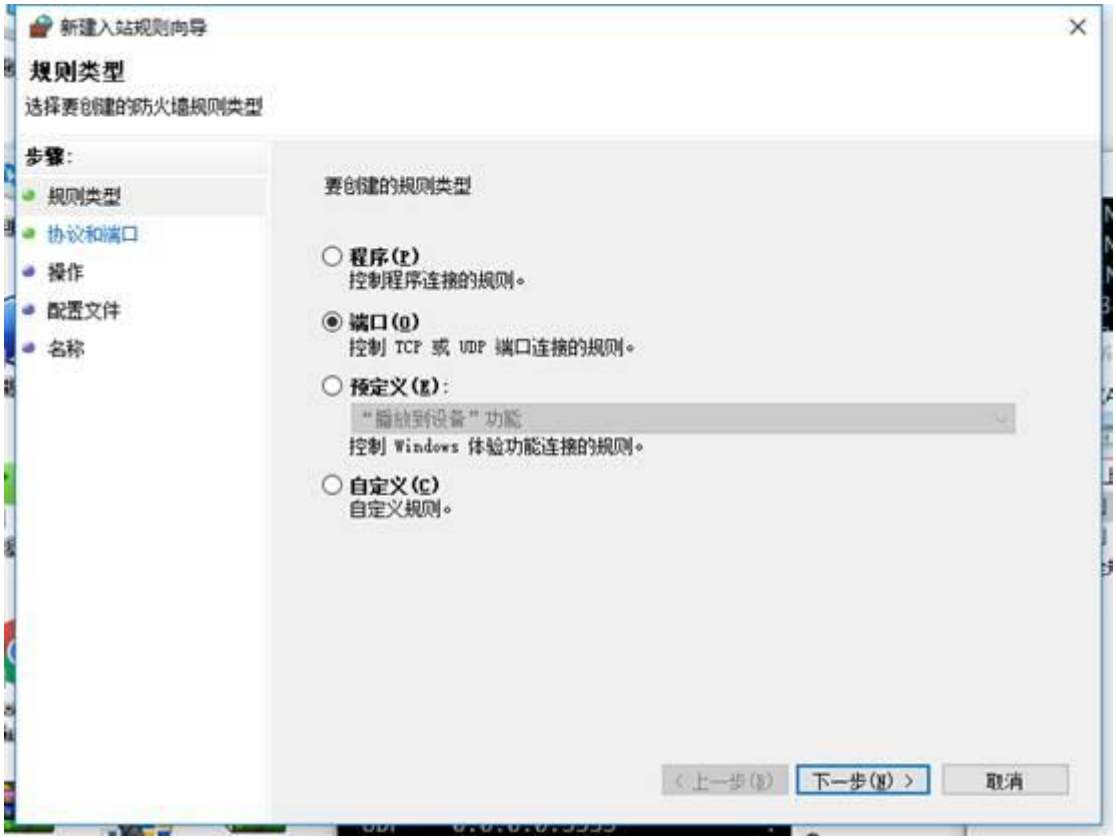
2、选择启动防火墙，并点击确定

3、点击高级设置

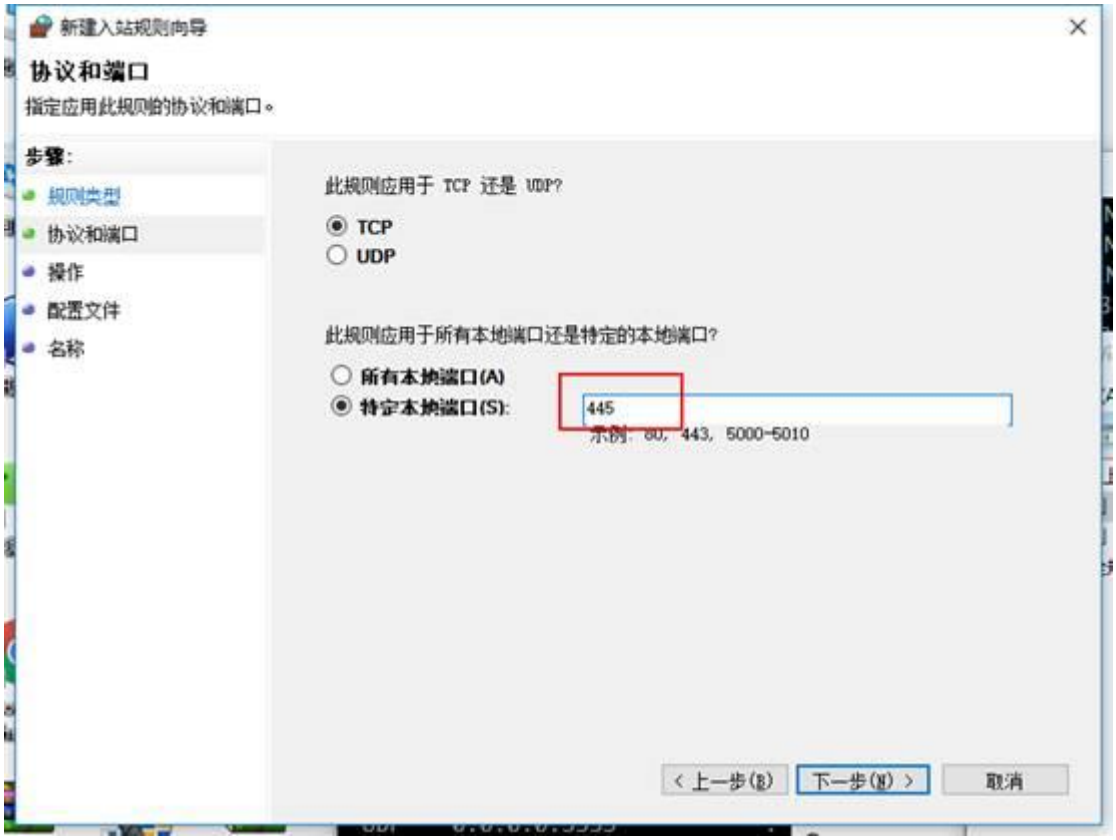
4、点击入站规则，新建规则



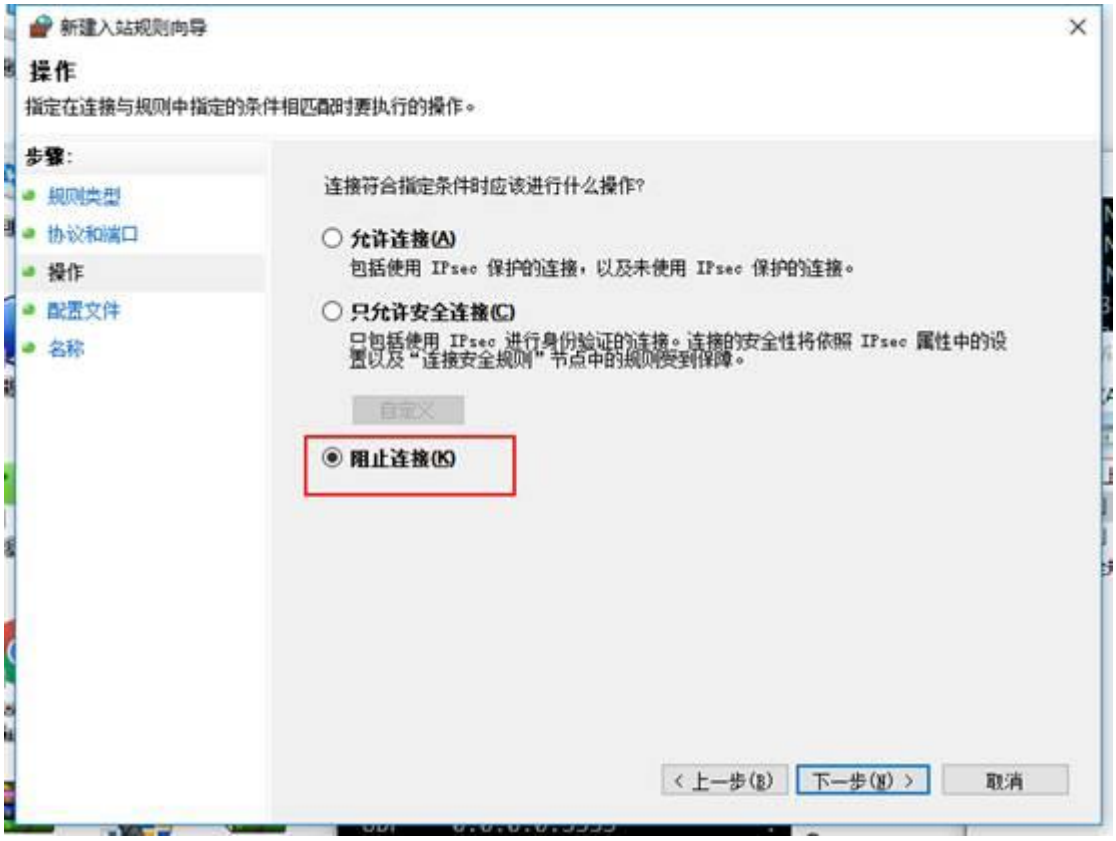
5、选择端口，下一步



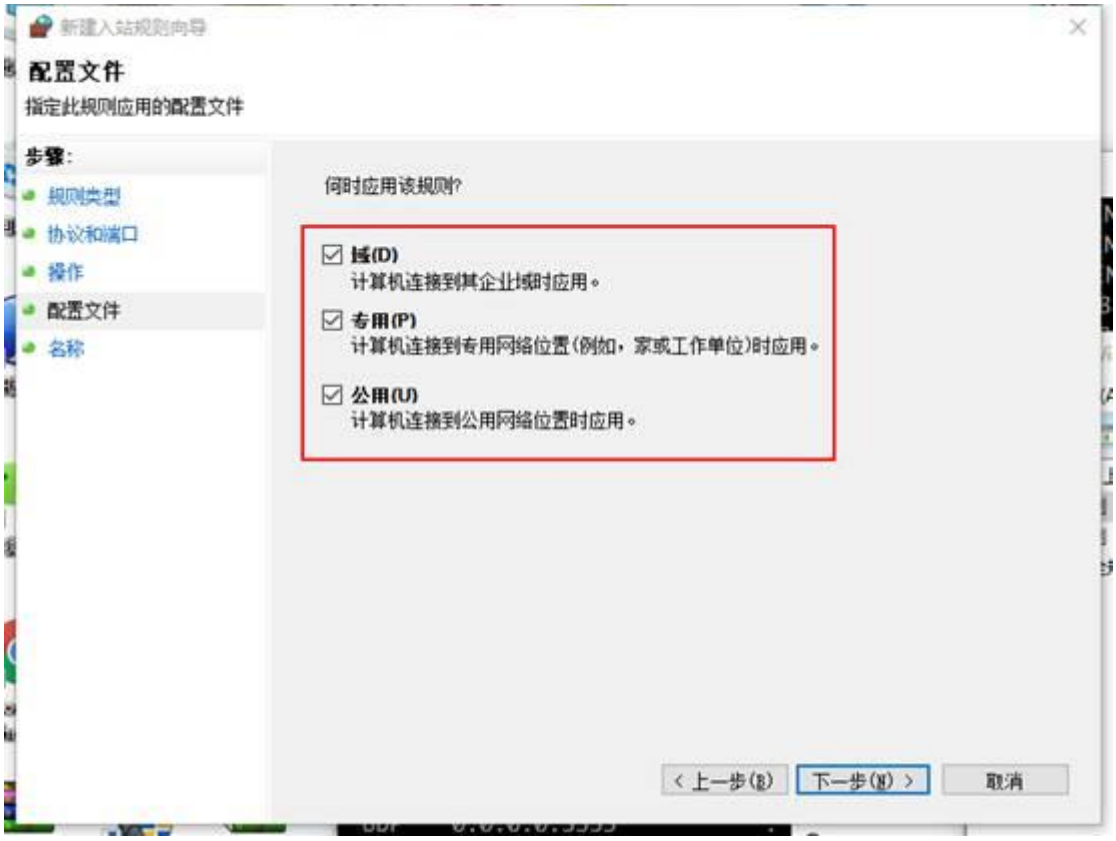
6、特定本地端口，输入 445，下一步


新建入站规则向导
协议和端口
指定应用此规则的协议和端口。
步骤:
规则类型
协议和端口
操作
配置文件
名称
此规则应用于 TCP 还是 UDP?
TCP
UDP
此规则应用于所有本地端口还是特定的本地端口?
所有本地端口(A)
特定本地端口(S):
445
示例: 80, 443, 5000-5010
< 上一步(B)
下一步(N) >
取消

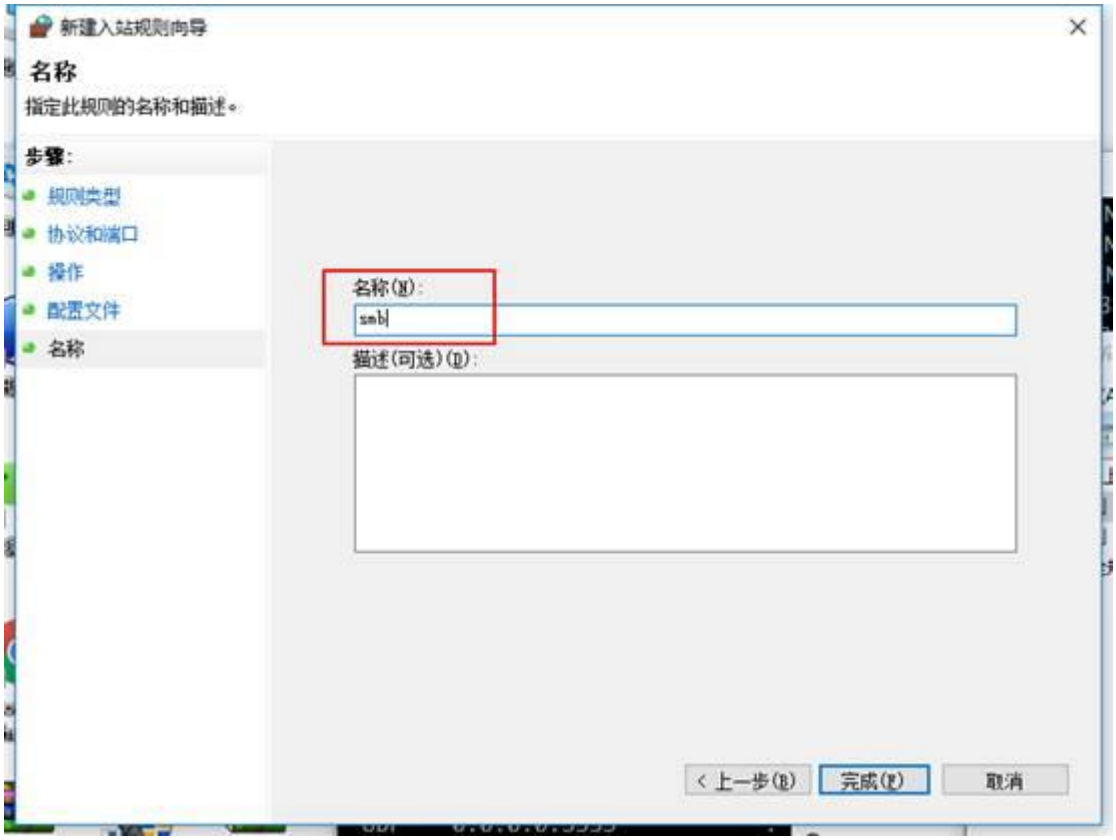
7、选择阻止连接，下一步


新建入站规则向导
操作
指定在连接与规则中指定的条件相匹配时要执行的操作。
步骤:
规则类型
协议和端口
操作
配置文件
名称
连接符合指定条件时应该进行什么操作?
允许连接(A)
包括使用 IPsec 保护的连接，以及未使用 IPsec 保护的连接。
只允许安全连接(C)
只包括使用 IPsec 进行身份验证的连接。连接的安全性将依照 IPsec 属性中的设置以及"连接安全规则"节点中的规则实到保障。
自定义...
阻止连接(K)
< 上一步(B)
下一步(N) >
取消

8、配置文件，全选，下一步

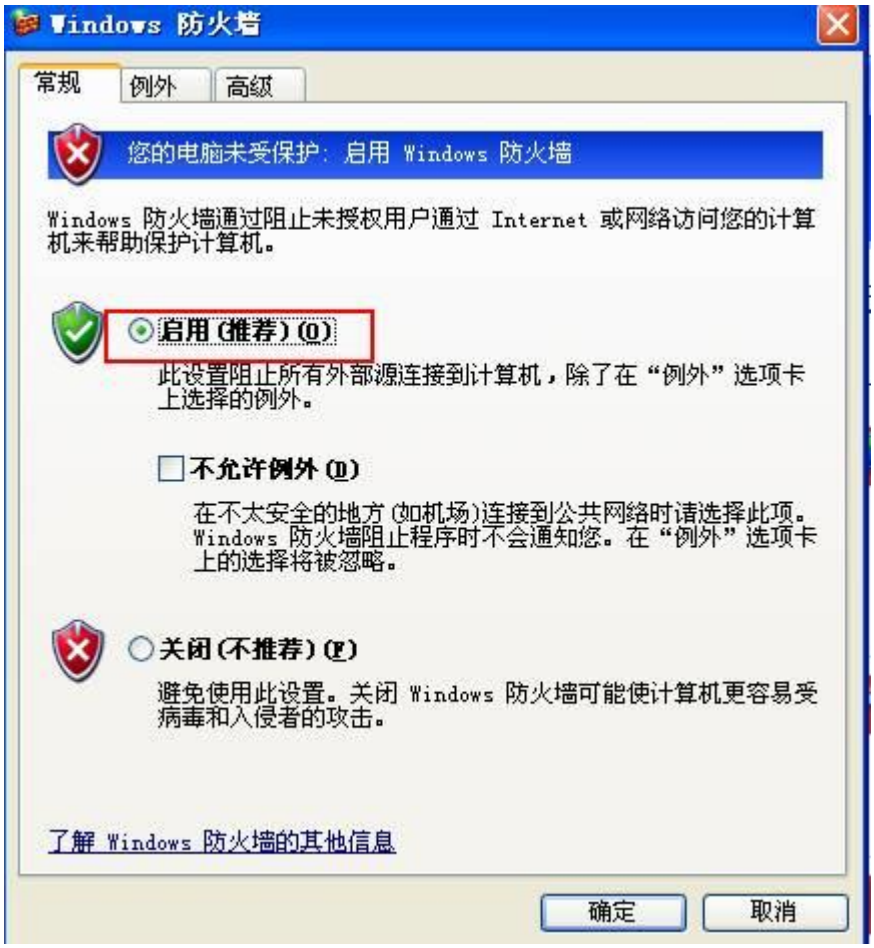


9、名称，可以任意输入，完成即可。



方法二、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（**此命令在执行前应先确认是否有应用程序需要用到相关端口服务**）

```
net stop rdr
net stop srv
net stop netbt
```

3、由于微软已经不再为 XP 系统提供系统更新，建议尽快升级到高版本系统。对于本次漏洞，由于危害巨大，微软提供了 WinXp 和 Win2003 的特别补

丁，下载地址如下：

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

本次事件技术支撑易信群：

中国电信股份有限公司上海分公司

2017 年 5 月 14 日