2017 年 05 月

永恒之蓝防护方案
应急通告

2017 年 05 月 13 日稿

Venusense

Situation Awareness

目录

一. 核心结论

正值我国“一带一路”全球化会议召开期间，北京时间 2017 年 5 月 12 日晚 20 时左右，在国内大规模爆发勒索攻击，我国大量金融机构、企业、教育网遭受冲击。

勒索攻击名为“wannacry、ONION、Wncry”是早前披露 NSA 黑客武器库泄漏的“永恒之蓝”发起的攻击事件，目前无法解密该勒索软件加密的文件。磁盘感染后，文件会被加密为.onion 后缀，只有支付高额赎金才能解密恢复文件，对重要数据造成严重损失。

攻击行为会扫描开放 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，攻击者就能在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。

由于以前国内多次爆发利用 445 端口传播的蠕虫，部分运营商在主干网络上封禁了 445 端口，但是教育网并没有此限制，仍然存在大量暴露 445 端口且存在漏洞的电脑，导致目前此蠕虫在教育网内大量传播，大概量级是每天 5000 个用户中招。

该勒索攻击迅速感染的原因是利用了基于 445 端口传播扩散的“SMB 漏洞 MS17-101”，微软在今年 3 月份发布了该漏洞的补丁，补丁链接下：

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

防护的有效性最终会体现在与攻击者的对抗过程，尽管这次事件带来的损失可能十分惨痛，但能够警醒所有信息管理者，这种后果严重的大规模灾难本质上是一种浅层次风险造成的后果，相对更为深度、隐蔽风险，这些浅层次风险有效完善纵深防御体系和执行能力更是日常信息安全工作的重中之重。

完善解决方案咨询，可联系我们！

二. 永恒之蓝防御措施

2.1 影响范围

此次利用的 SMB 漏洞影响以下未自动更新的操作系统：

Windows XP、Windows 2000、Windows 2003

Windows Vista、Windows Server 2008、Windows Server 2008 R2

Windows 7、Windows 8、Windows 10

Windows Server 2012、Windows Server 2012 R2、Windows Server 2016

注：以下设备不受影响

安卓手机，iOS 设备，MacOS 设备，*nix 设备、Win10 用户如果已经开启自动更新不受影响。

2.2 解决办法

2.2.1 网络侧应急解决方案

- ✧ 在边界出口交换路由设备禁止外网对内网 135/137/139/445 端口的连接。
- ✧ 在内网核心主干交换路由设备禁止 135/137/139/445 端口的连接。
- ✧ 如果有部署入侵防御等防护系统则尽快检查漏洞库升级，开启防御策略。
- ✧ 发布通知重点留意邮件、移动存储介质等传播渠道，做好重点检查防护工作。

2.2.2 终端侧应急解决方案

注：请扫描内网，发现所有开放 445 SMB 服务端口的终端和服务器，对于 Win7 及以上版本的系统确认是否安装了 MS07-010 补丁，如没有安装则受威胁影响。Win7 以下的 Windows XP/2003 目前没有补丁，只要开启 SMB 服务就受影响。

```
C:\Users\Administrator>netstat -ano |findstr 445
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    192.168.0.101:14445    116.228.159.53:443     LAST_ACK        16644
  TCP    192.168.0.101:14450    116.228.159.53:443     LAST_ACK        16644
  TCP    [::]:445               [::]:0                 LISTENING       4
```

1) 利用本地防火墙阻挡防护

✓ 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

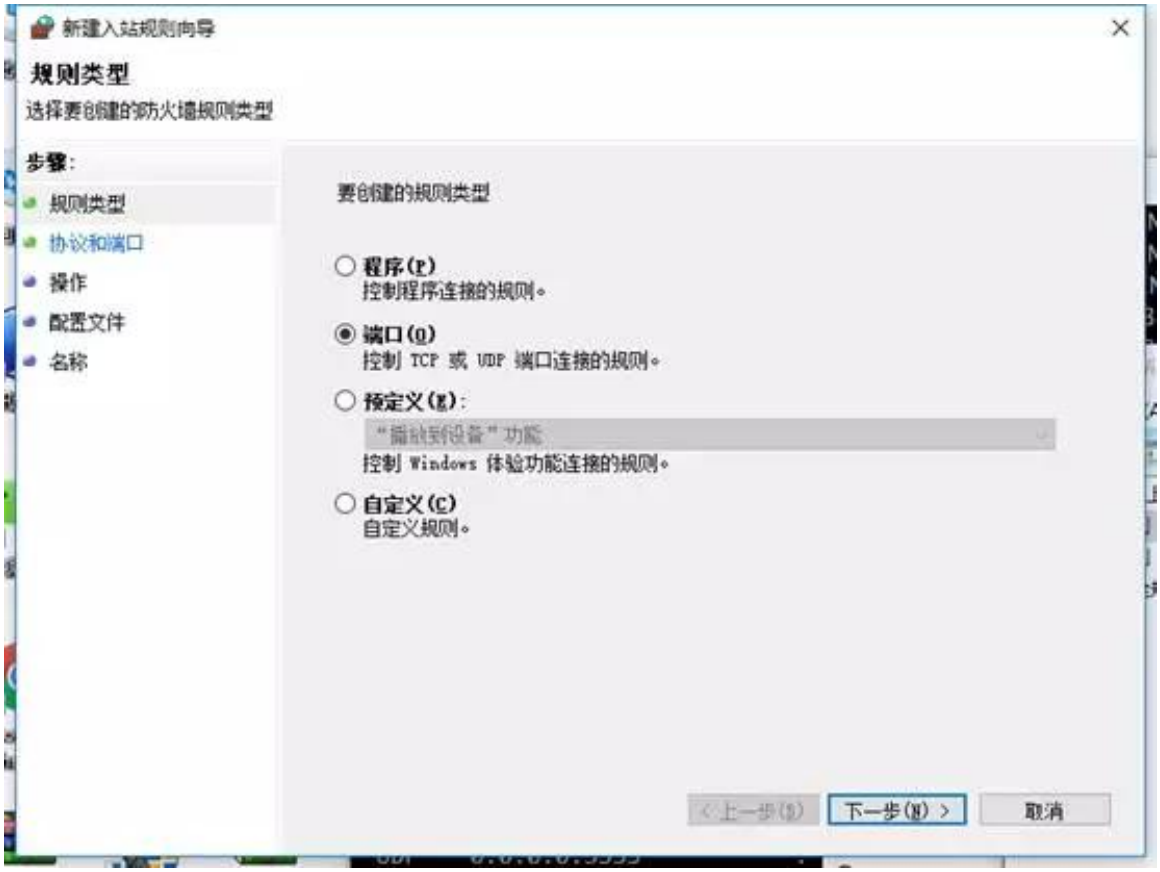

自定义各类网络的设置
你可以修改使用的每种类型的网络的防火墙设置。
专用网络设置
启用 Windows 防火墙
阻止所有传入连接，包括位于允许应用列表中的应用
Windows 防火墙阻止新应用时通知我
关闭 Windows 防火墙(不推荐)
公用网络设置
启用 Windows 防火墙
阻止所有传入连接，包括位于允许应用列表中的应用
Windows 防火墙阻止新应用时通知我
关闭 Windows 防火墙(不推荐)
确定
取消

3、点击高级设置

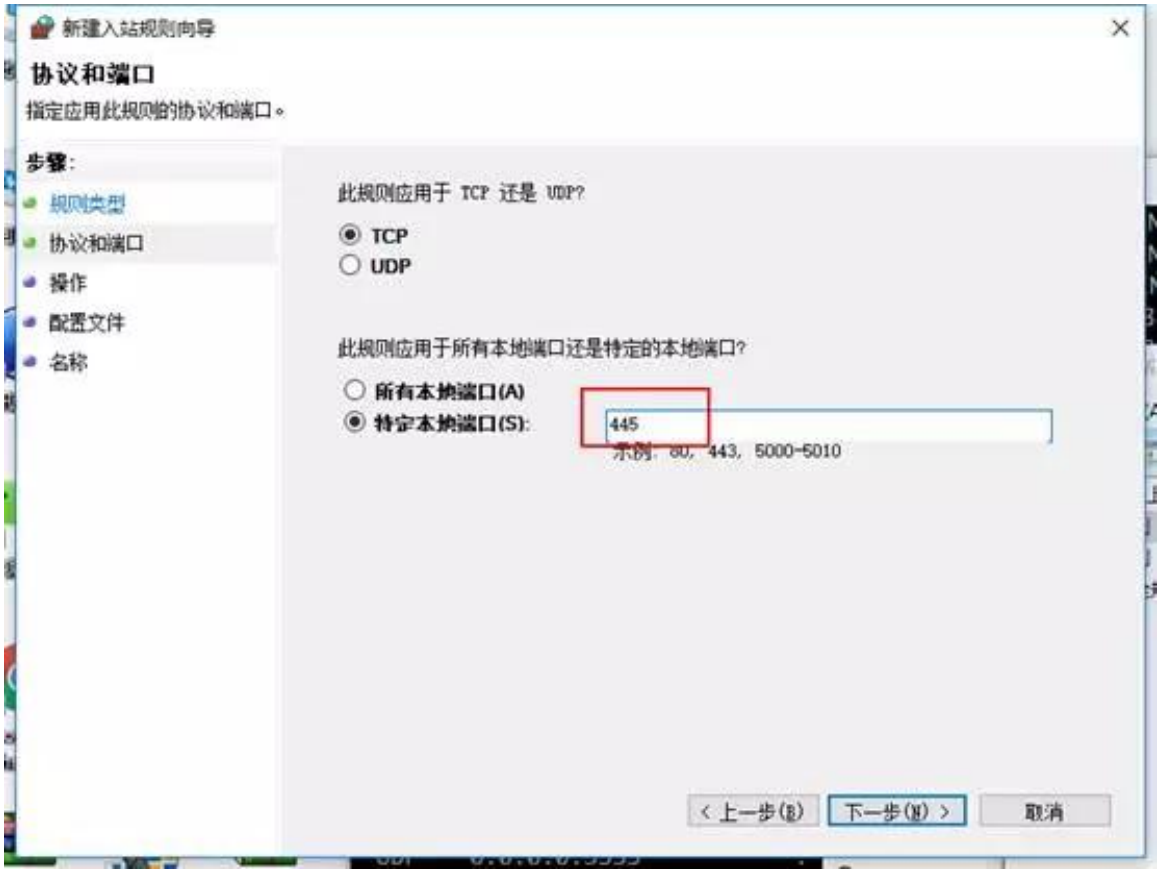

Windows 防火墙
控制面板 › 系统和安全 › Windows 防火墙
控制面板主页
允许应用或功能通过 Windows 防火墙
更改通知设置
启用或关闭 Windows 防火墙
还原默认值
高级设置
对网络进行疑难解答
使用 Windows 防火墙来帮助保护你的电脑
Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电
专用网络(R)
来宾或公用网络(P)
公共场所(例如机场或咖啡店)中的网络
Windows 防火墙状态:
启用
传入连接:
阻止所有与未在允许应
活动的公用网络:
网络
通知状态:
Windows 防火墙阻止新

4、点击入站规则，新建规则

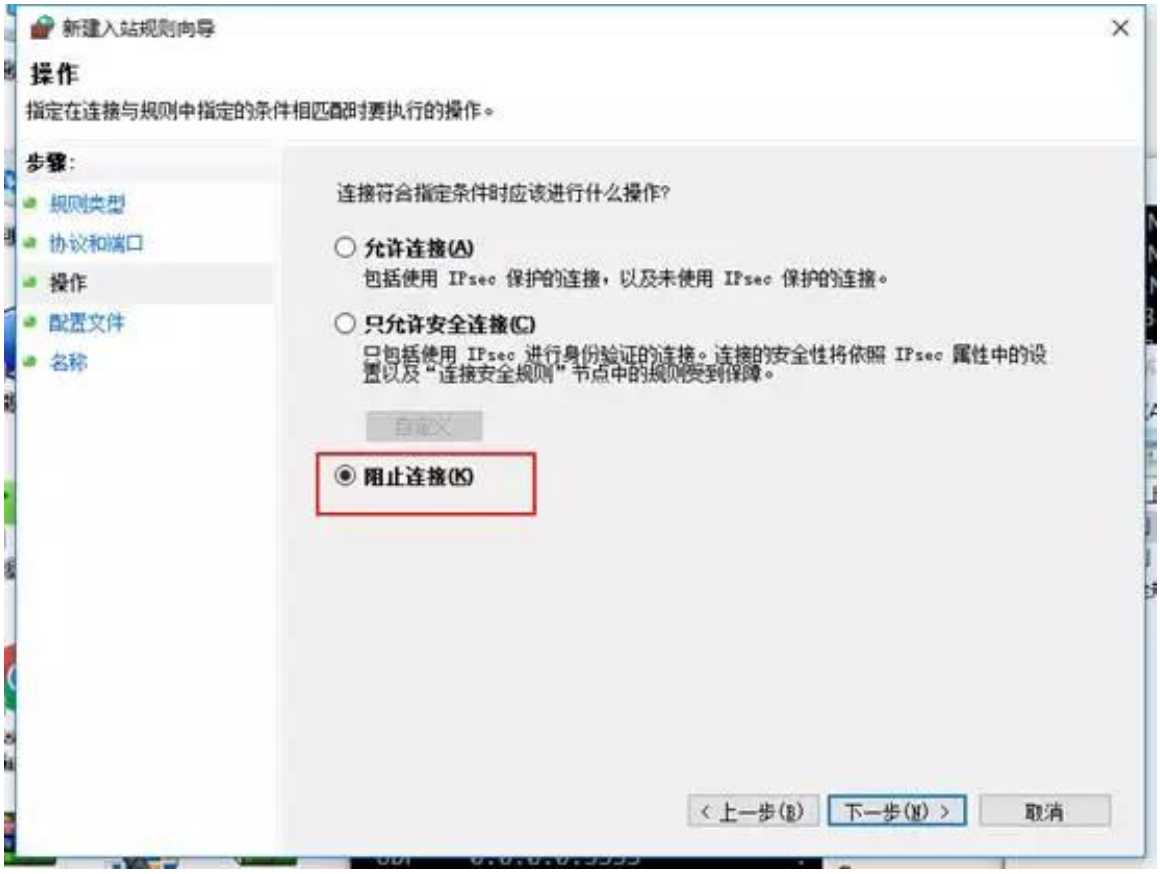
5、选择端口，下一步



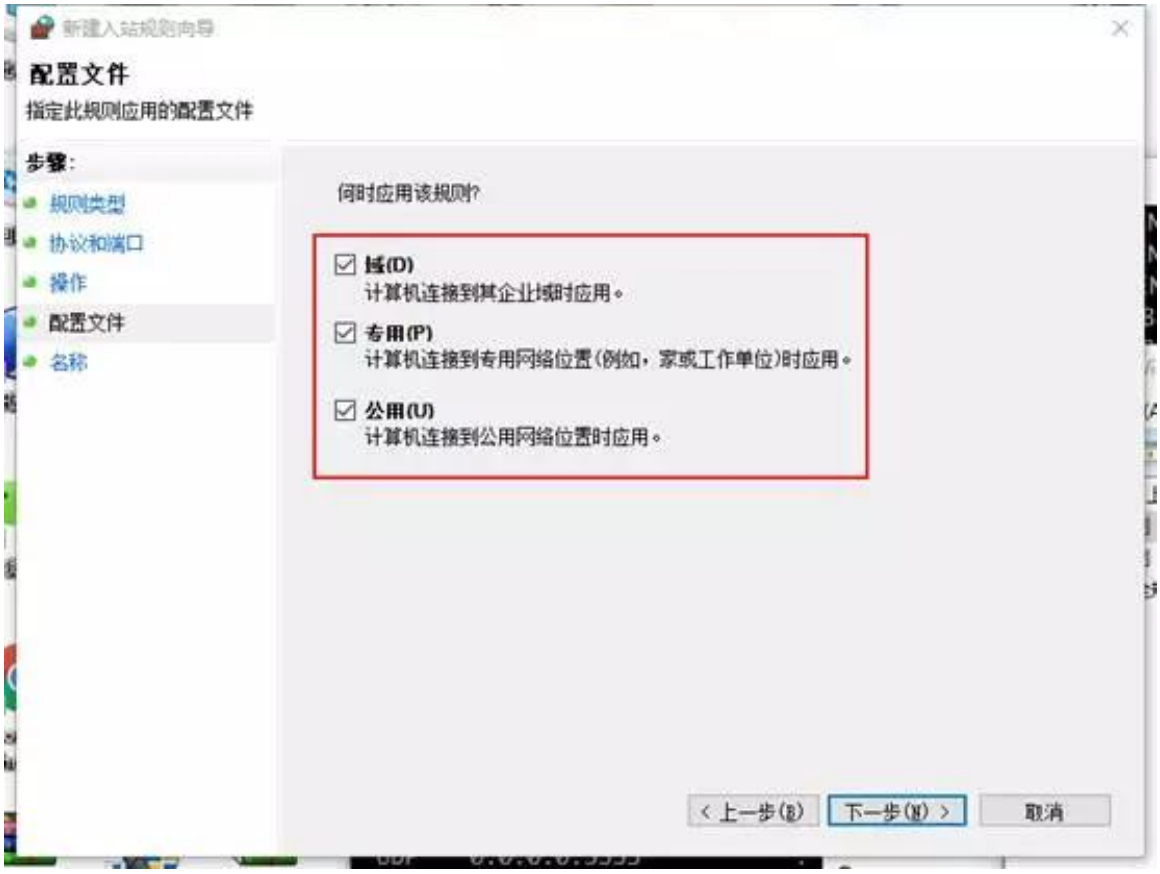
6、特定本地端口，输入 445，下一步


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

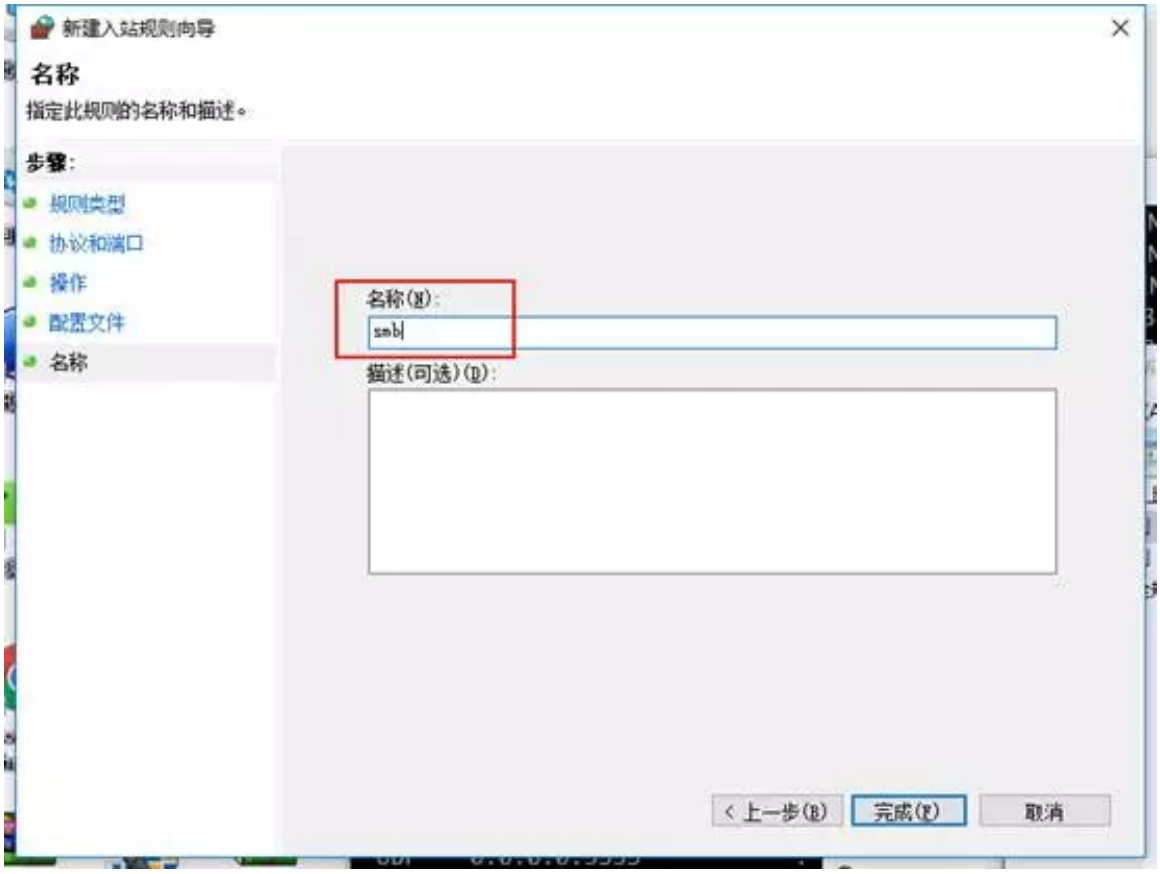
7、选择阻止连接，下一步


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”节点中的规则受到保障。
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

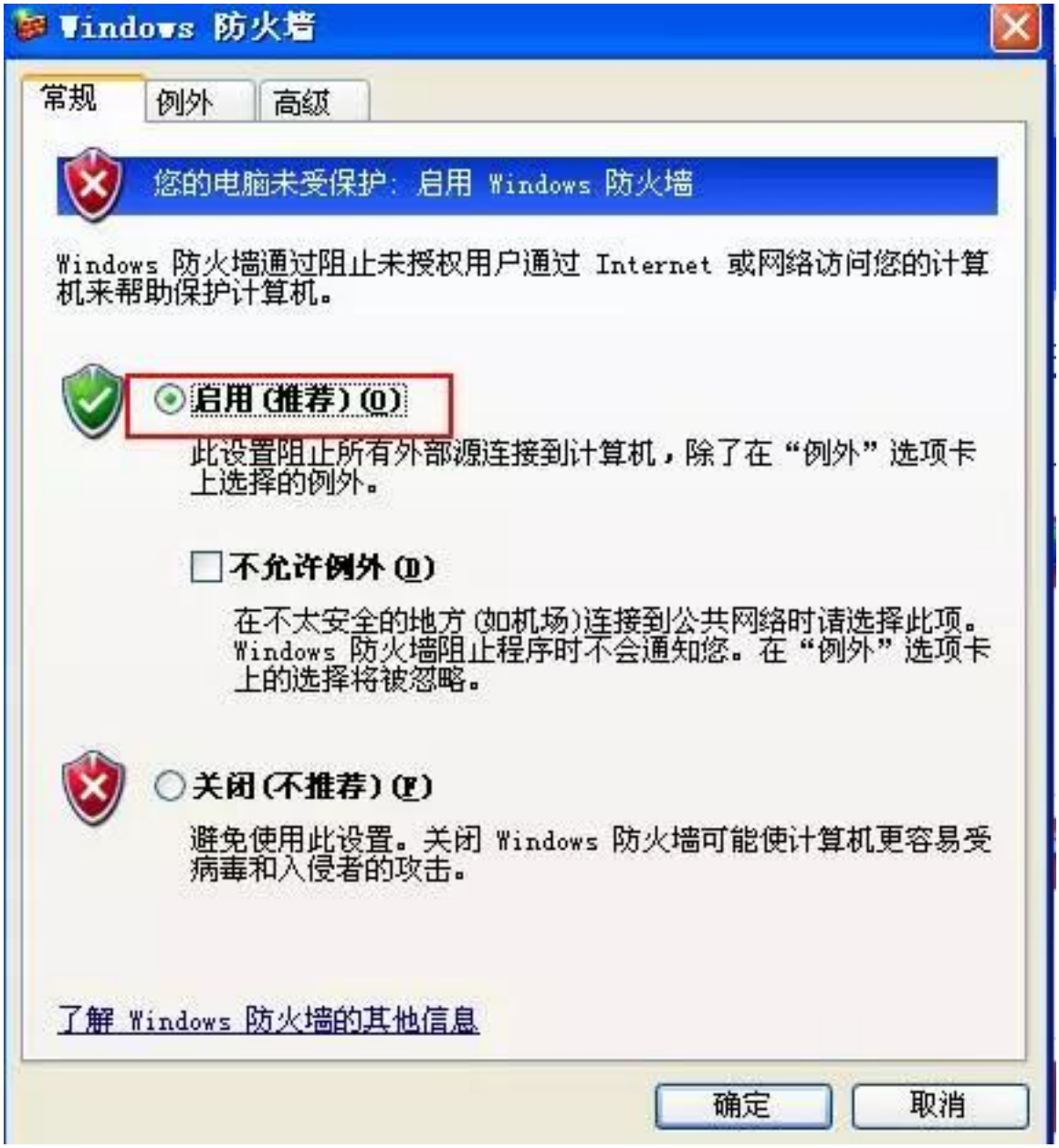


9、名称，可以任意输入，完成即可。



✓ 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

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

2) 手动下载安装补丁

补丁下载地址

win7 :https://mirror.sdu.edu.cn/ms17-010/win7/

win8 :https://mirror.sdu.edu.cn/ms17-010/win8/

请根据自己电脑的位数下载.

2.2.3 主动扫描发现漏洞的安全建议

“永恒之蓝”勒索蠕虫的检查，漏扫产品已经全面支持，请大家升级至最新漏洞库即可，建议使用漏扫 6070、网御漏洞扫描系统 V6.0 以上版本进行扫描，最新漏洞库 607000088。原 6061 版本同步支持，最新漏洞库 6000505 （6061 需使用授权扫描）

2.2.4 入侵事件库的更新建议

全面更新 IDS 或 NGIPS 的时间，以便应对“永恒之蓝”勒索攻击。

TCP_Windows_NSA_Pcdllluancher 工具执行成功

TCP_Windows_SMB 远程代码执行漏洞 NSA 工具_shellcode 植入

TCP_Windows_SMB_NSA_DoublePulsar 植入成功

MSRPC_Windows_SMB 远程代码执行漏洞_Eclipsdwing

MSRPC_Windows_SMB 远程代码执行漏洞_eclipsdwing1

TCP_windows_SMB 远程代码执行漏洞 ERRATICGOPHER

TCP_windows_SMB 远程代码执行漏洞 ERRATICGOPHER2

TCP_Windows_SMB 远程代码执行漏洞 EternalRomance[MS17-010]

TCP_windows_SMB 远程代码执行漏洞 ERRATICGOPHER1

TCP_Windows_SMB 远程代码执行漏洞 EternalBlue[MS17-010]

TCP_Windows_SMB 远程代码执行漏洞 CVE-2017-0144

参考链接：

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

https://github.com/x0rz/EQGRP_Lost_in_Translation/

2.2.5 已经感染设备应急解决方案

- ✧ 断开网络连接，组织进一步扩散。
- ✧ 优先检查未感染主机的漏洞状况（可直接联系启明星辰，提供免费检测工具使用），做好漏洞加固工作后方可恢复网络连接。

- ✧ 已经感染终端，根据终端数据类型决定处置方式，如果重新安装系统则建议完全格式化硬盘、使用新操作系统、完善操作系统补丁、通过检查确认无相关漏洞后再恢复网络连接。