

互联网网络安全信息通报

国家计算机网络应急技术处理协调中心广东分中心 5 月 13 日

1.概述



●

●

445

445

●

Win7 Win8 Win10

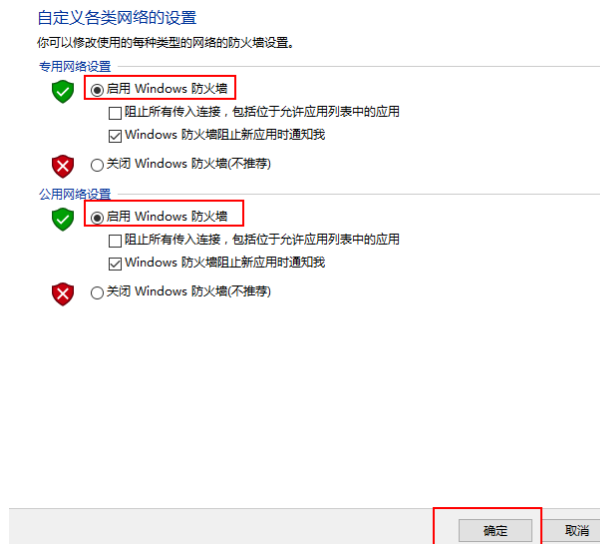
1)



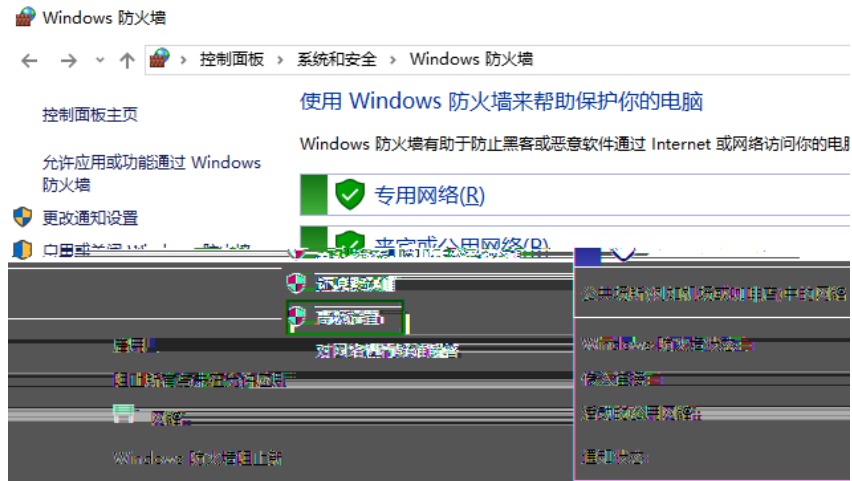
2) - Windows Windows



3)

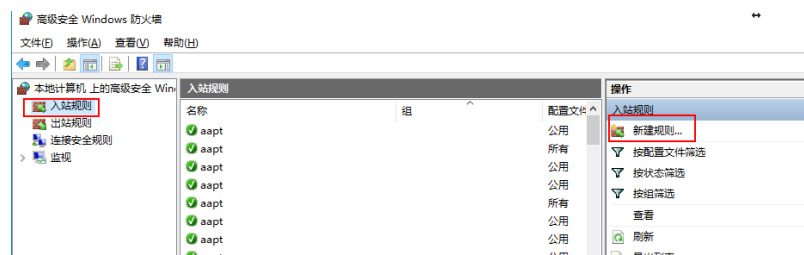


4)

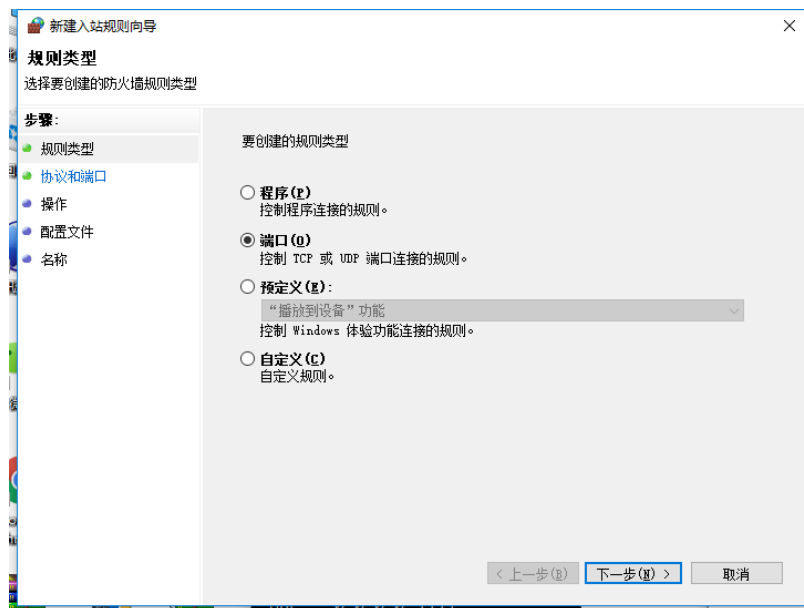


5)

445

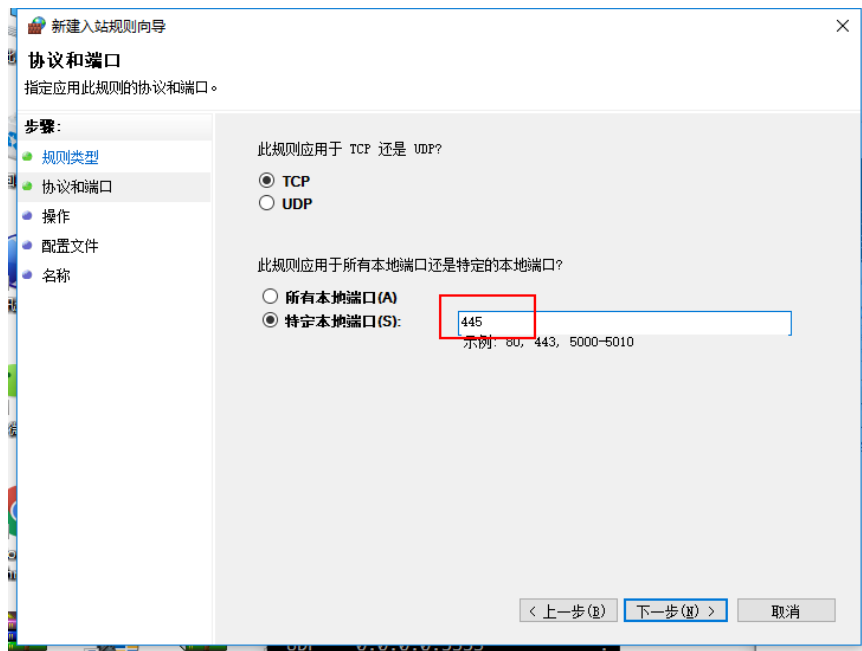


6)

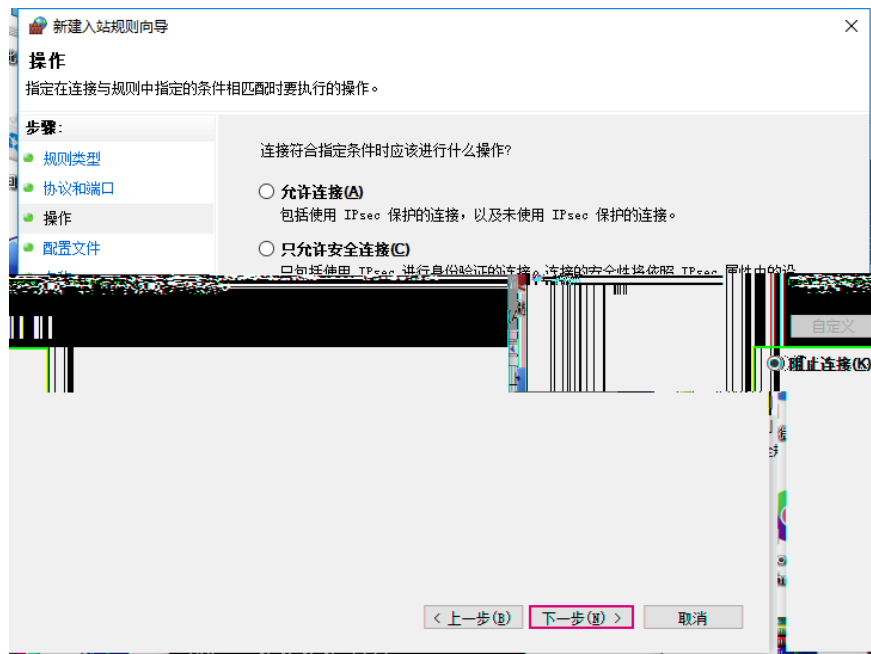


7)

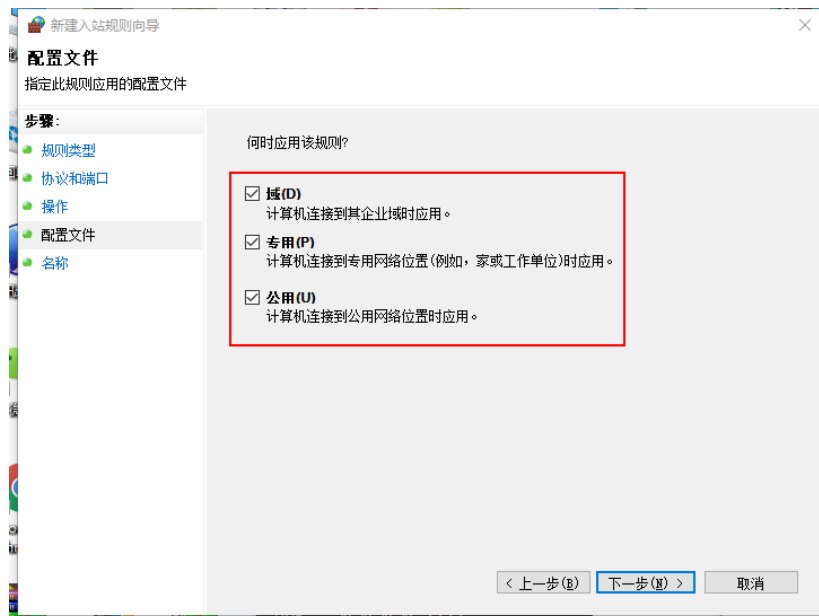
445



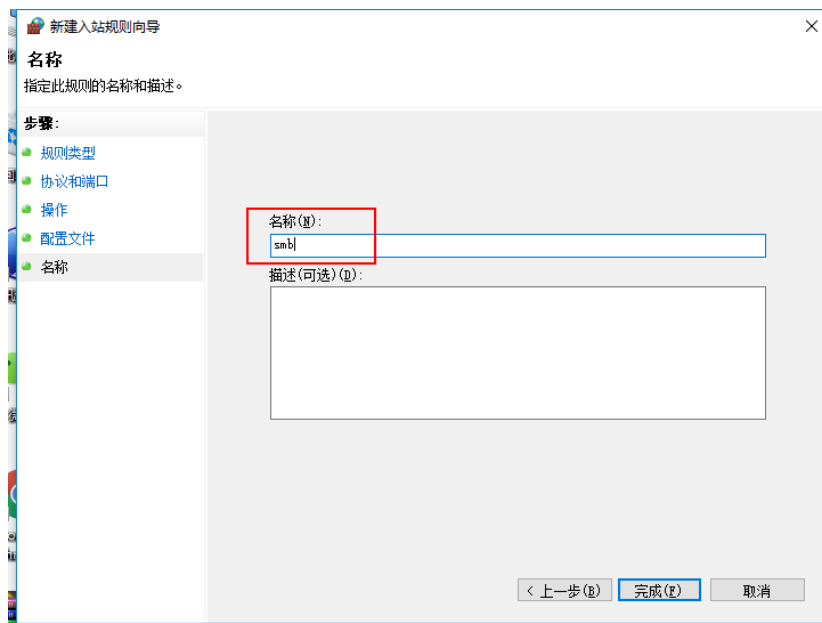
8)



9)



10)



11)

MS17-010

winxp_sp3

win10

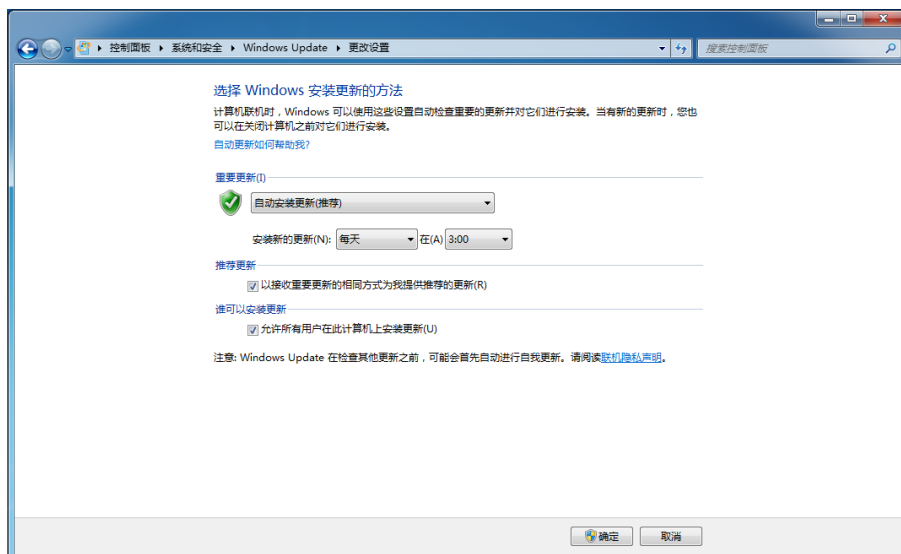
win2003

win2016

<https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/?from=timeline&isappinstalled=0>



12)

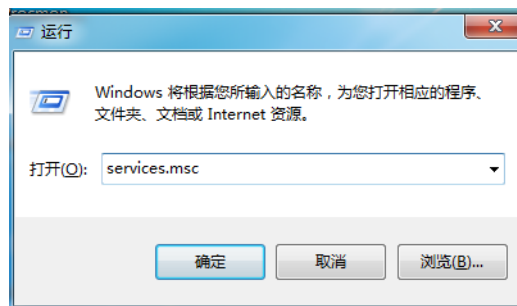


13) Win7

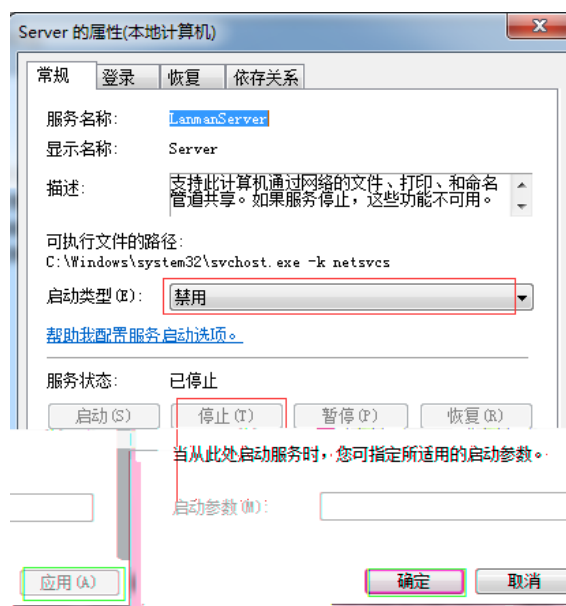
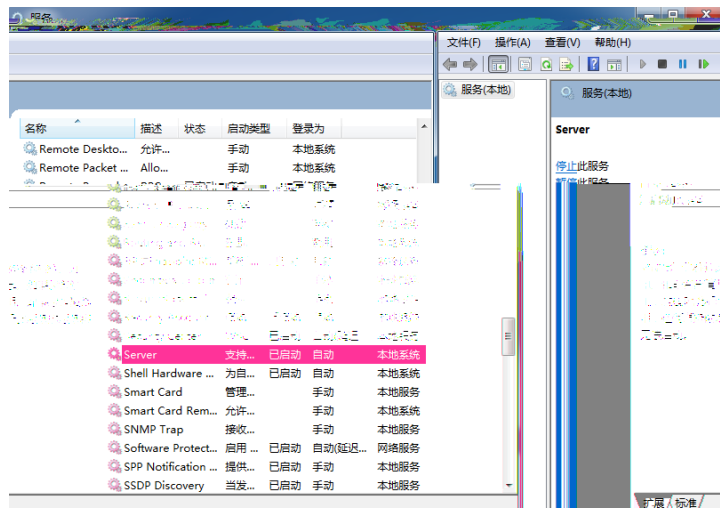
Server
server

445

services.msc



Server

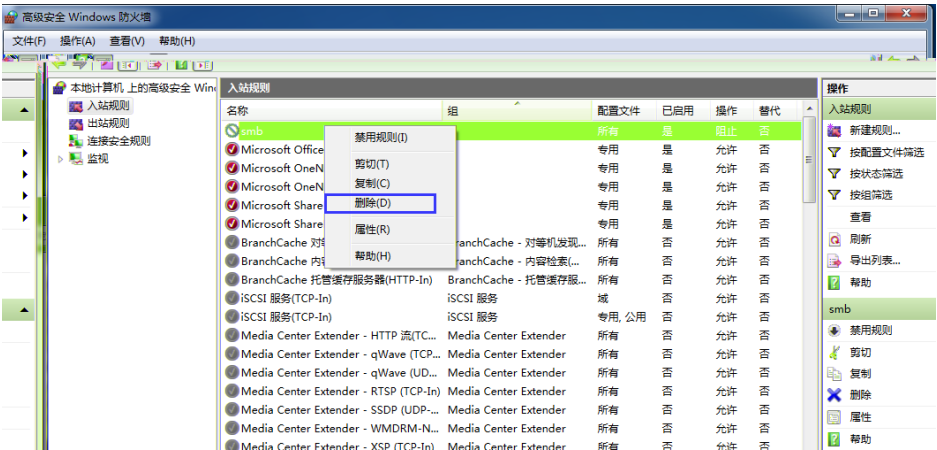


win7 netstat an 445

```
C:\Users\...>netstat -an

活动连接
 协议 本地地址           外部地址           状态
TCP    0.0.0.0:135         0.0.0.0:0          LISTENING
TCP    0.0.0.0:5357        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49152       0.0.0.0:0          LISTENING
TCP    0.0.0.0:49153       0.0.0.0:0          LISTENING
TCP    0.0.0.0:49154       0.0.0.0:0          LISTENING
```

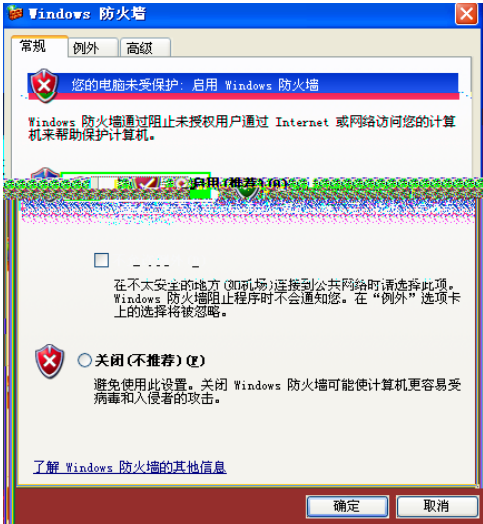
SMB



Win

1)

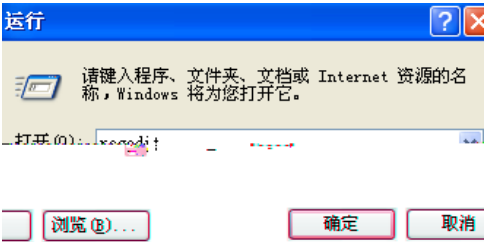
Windows



2)

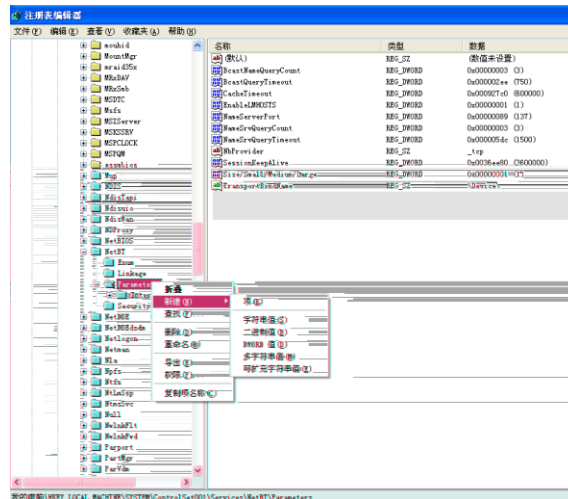
445

regedit

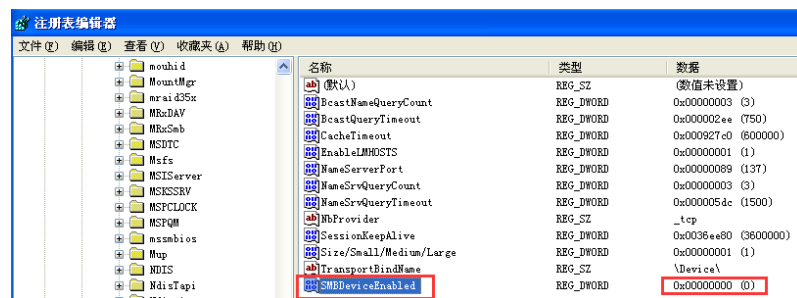


3)

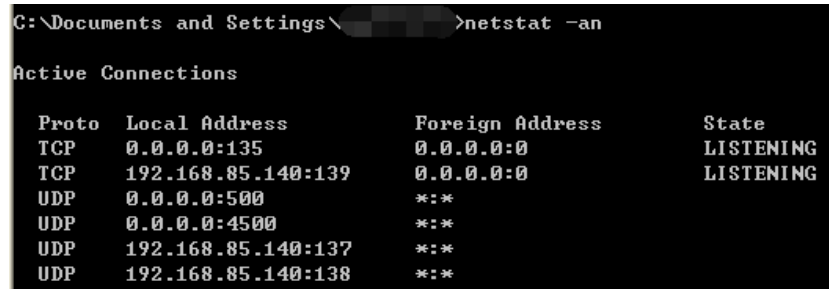
HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters
Parameters
DWORD



4) DWORD SMBDeviceEnabled 0



5) 445



6) Wannacry XP

<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wanna-crypt-attacks/>



NSA武器库免疫工具

- 该漏洞危害可以远程攻破全球约70%Windows机器
- 该漏洞危害不需要用户任何操作，只要联网就可以远程攻击

! 经检测，发现您的电脑存在该漏洞，请立即修复!

- EternalBlue (永恒之蓝)
- EternalChampion (永恒王者)
- EternalRomance (永恒浪漫)
- EternalSynergy (永恒协作)
- EmeraldThread (翡翠纤维)
- ErraticGopher (古怪地鼠)
- EskimoRoll (爱斯基摩卷)
- EducatedScholar (文雅学者)
- EclipsedWing (日食之翼)
- EsteemAudit (尊重审查)

立即修复

通过360安全卫士安装补丁

