Windows10系统关闭高危端口方法简介

Windows10默认开启一些日常用不到的端口，这些端口让黑客有机可乘（黑客会使用工具扫描计算机上的端口，并入侵这些端口），关闭这些高危端口，可使我们的电脑避免遭受攻击。例如关闭445端口等，可有效防止勒索病毒。

一、部分端口简单介绍

日常的Windows或Linux，甚至一些高端的路由器都有高危端口，建议配置完成后关闭端口或者开启访问控制权限，这样可以防止一些不必要的黑客骚扰。部分端口如下：

20：FTP服务数据连接端口。

21：FTP服务控制连接端口。

22：SSH服务端口，建议更换。

23：Telnet服务端口，远程登录。

53：DNS解析服务端口。

67：DHCP Server服务端口。

68：DHCP Client服务端口。

69：TFTP服务端口。

80：WWW服务端口。

110：POP3服务端口，接收邮件。

135：RPC服务端口，永恒之蓝。

137端口：NetBIOS名称服务，永恒之蓝。在局域网中提供计算机的名字或IP地址查询服务，一般安装了NetBIOS协议后，该端口会自动处于开放状态。要是非法入侵者知道目标主机的IP地址，并向该地址的137端口发送一个连接请求时，就可能获得目标主机的相关名称信息。例如目标主机的计算机名称，注册该目标主机的用户信息，目标主机本次开机、关机时间等。此外非法入侵者还能知道目标主机是否是作为文件服务器或主域控制器来使用。

138：共享服务端口，永恒之蓝。

139端口：NetBIOS/SMB服务端口，永恒之蓝。为“NetBIOS Session Service”提供的，主要用于提供Windows文件和打印机共享以及Unix中的Samba服务。开启139端口虽然可以提供共享服务，但是常常被攻击者所利用进行攻击，比如使用流光、SuperScan等端口扫描工具，可以扫描目标计算机的139端口，如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的。

143：IMAP服务端口，接收邮件。

161：SNMP服务端口。

162：SNMP服务端口。

443：WWW服务端口，Https网页。

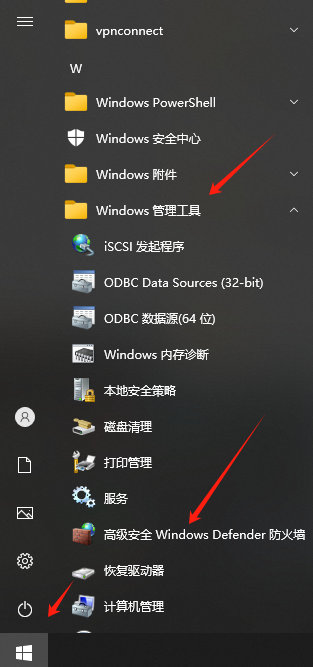
445端口：文件共享端口，永恒之蓝。445端口是一个毁誉参半的端口，有了它我们可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机，他们能通过该端口偷偷共享你的硬盘，甚至会在悄无声息中将你的硬盘格式化掉。2017年10月，由于病毒“坏兔子”来袭，国家互联网应急中心等安全机构建议用户及时关闭计算机以及网络设备上的445和139端口。

1194：Open VPN服务端口。

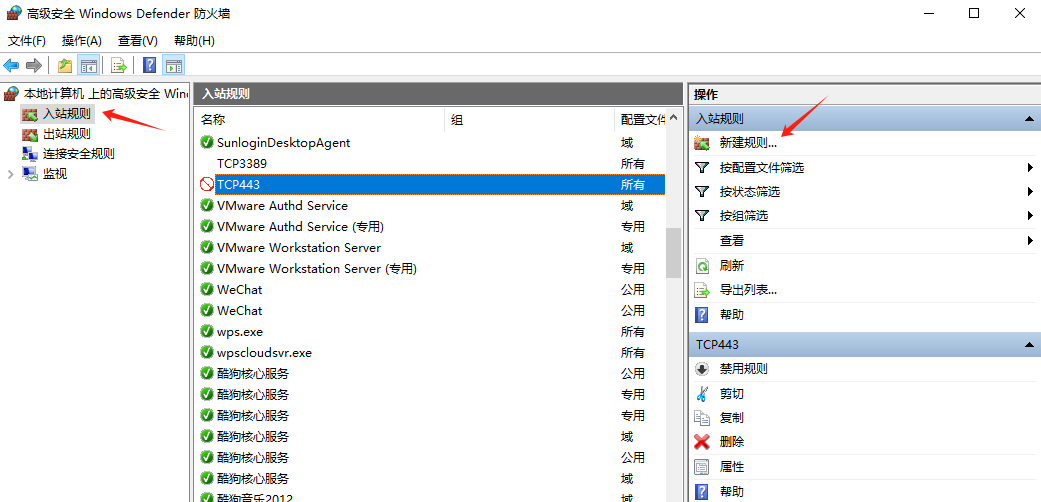
3306：MySQL数据库端口。

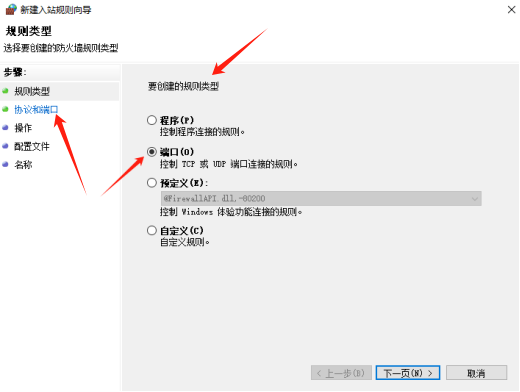
3389：远程桌面。

二、Windows10 系统关闭非必要端口操作步骤

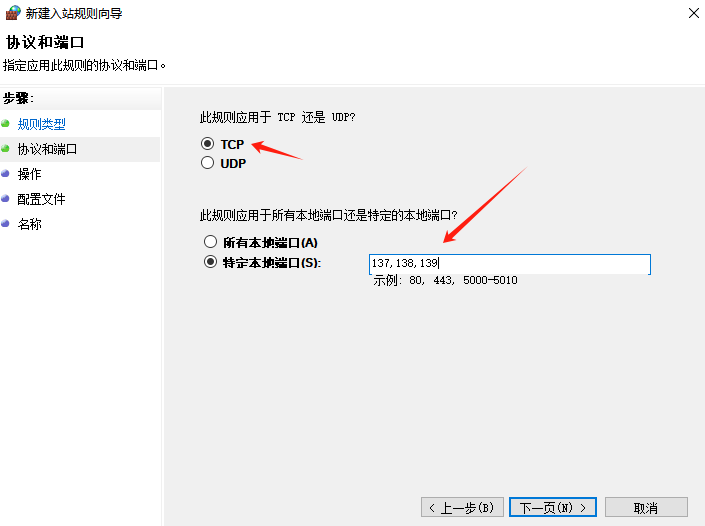
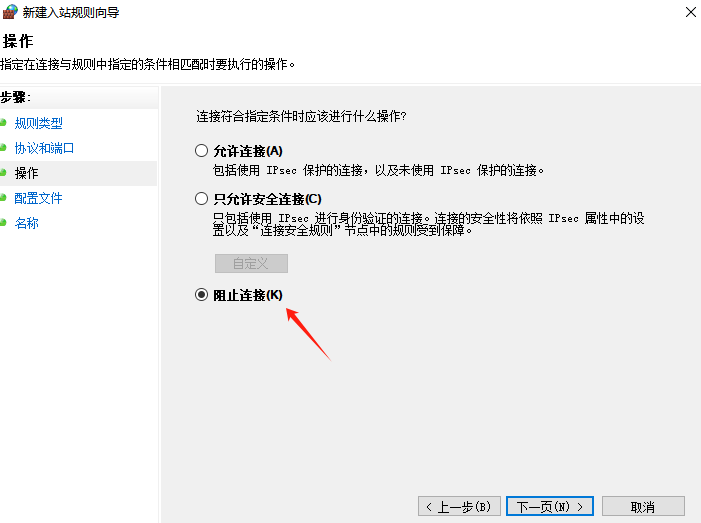
1、点击**开始**图标，选择点击**Windows管理工具**，选择点击**高级安全Windows Defender防火墙**。

2、在高级安全Windows Defender防火墙页面，选择**入站规则**，点击**新建规则**。

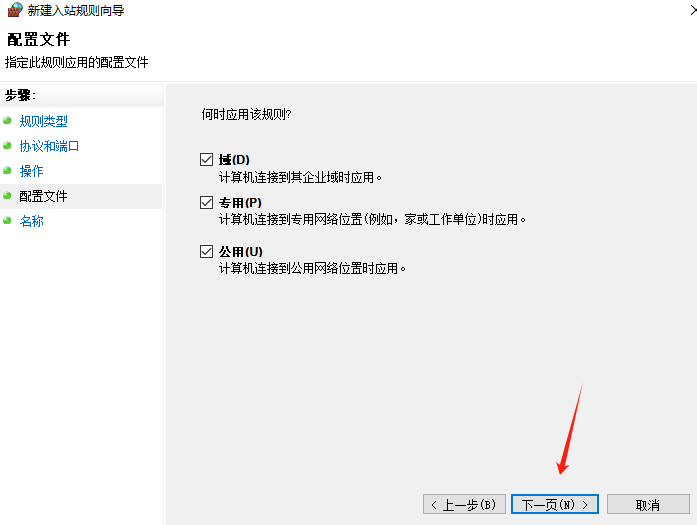
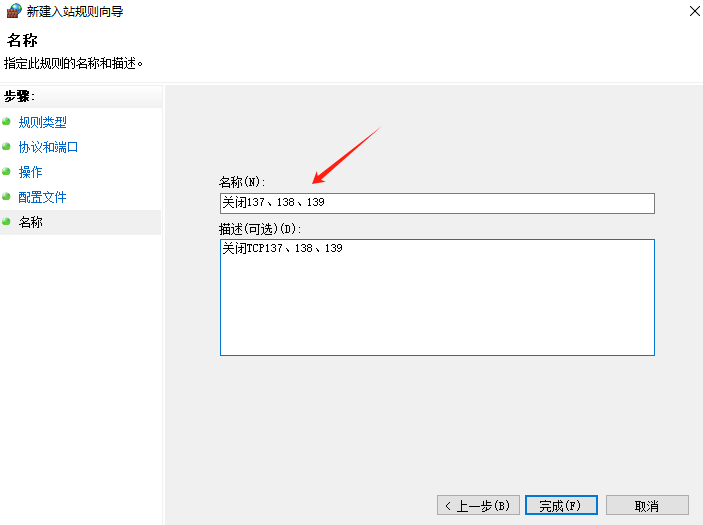
3、在新建入站规则向导页面，点击**协议和端口**，选择要创建的规则类型，点击**端口（o）**按钮，点击下一页。

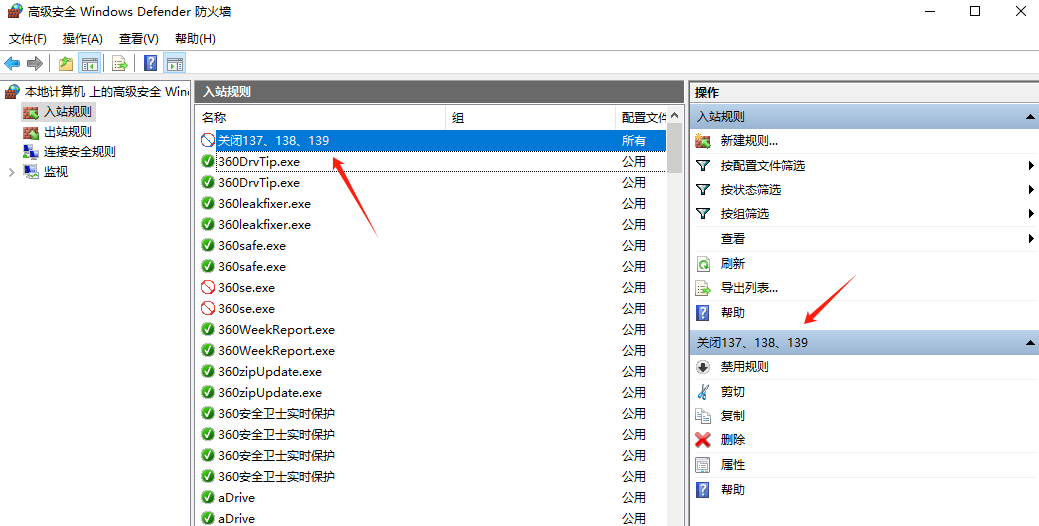


4、在**此规则应用于TCP还是UDP** 页面,**先选择TCP（再选择UDP，见步骤9）**,选择**特定本地端口（s）**，输入要关闭的端口号（如**22,137,138,139,445**等）,中间用逗号隔开，特别注意这里的逗号一定是英文的逗号。

5、点击**阻止连接**,点击**下一页**。

6、默认选择，点击**下一页**。

7、编辑名称如：“**关闭137、138、139**”，也可以添加一些描述相当于备注，点击**完成**。

8、在**高级安全Windows Defender防火墙**页面，查看**入站规则**，可以看到阻止连接的本地端口是之前设置的137,138,139，说明网络端口137,138,139已经阻止连接。

**9、重复关闭端口的步骤，在此规则应用于TCP还是UDP 页面中，选择UDP，再进行一次所有操作。**

**10、关闭端口后的示例如下图。**

