

Windows系统安全从定制IP策略开始 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/0/2021_2022_Windows_E7_B3_BB_c99_476.htm

现如今病毒、木马攻击的方式是多种多样，尤其是计算机端口更是病毒“攻占”的重点部位，你是否曾遇到这样的情况，当我们安装上诸如天网防火墙上网时，只见感叹号跳个不停。打开一看都是类似于“xxx.xxx.xxx.xxx 试图连接本机的xxx端口，该操作被拒绝”之类的操作提示，这就是一些病毒、木马攻击端口的表现。概念常识在上述情况进行解决之前，我们先要对一些常识性概念进行一番了解，尤其是涉及到端口方面的知识。什么是端口？在网络技术中，端口（Port）大致有两种意思：一是物理意义上的端口，比如，ADSL Modem、集线器、交换机、路由器用于连接其他网络设备的接口，如RJ-45端口、SC端口等等。二是逻辑意义上的端口，一般是指TCP/IP协议中的端口，端口号的范围从0到65535，比如用于浏览网页服务的80端口，用于FTP服务的21端口等等。本文所讲的端口指的是逻辑意义上的端口，它是计算机和外部网络相连的逻辑接口，也是计算机的第一道屏障。默认情况下，Windows有很多端口是开放的，上网的时候，网络病毒和黑客可以通过这些端口连上你的电脑。为了让你的系统变为铜墙铁壁，我们除了一些重要的端口，如80端口为Web网站服务；21端口为FTP服务；25端口为E-mail SMTP服务；110端口为E-mail POP3服务；1433端口为SQL Server服务等外，一些没有服务的端口都可以关闭，如TCP 135、139、445、593、1025 端口和 UDP 135、137、138、445 端口，一些流行病毒的后门端口（如 TCP 2745、3127

、6129 端口) ，以及远程服务访问端口3389等。对于一些没有服务的端口，除了使用一些网络防火墙来关闭外，借助IP安全策略来进行关闭可以说是一个阻止入侵者入侵的好办法，下面我们就来定制IP策略。

了解IP安全策略 IP安全策略是一个给予通讯分析的策略，它将通讯内容与设定好的规则进行比较以判断通讯是否与预期相吻合，然后决定是允许还是拒绝通讯的传输，它弥补了传统TCP/IP设计上的"随意信任"重大安全漏洞，可以实现更仔细更精确的TCP/IP安全，也就是说，当我们配置好IP安全策略后，就相当于拥有了一个免费，但功能完善的个人防火墙。

实战IP安全策略

- 1、创建一个IP安全策略
第一步：单击"开始"菜单，然后选择"设置 控制面板"，在弹出的"控制面板"中，双击"管理工具"图标，进入到"管理工具"中，再次双击其中的"本地安全策略"图标并进入到"本地安全策略"对话框中。
第二步：用鼠标右击"IP安全策略"，选择"创建IP安全策略"命令 在弹出的"IP安全策略向导"对话框中，单击"下一步"按钮，输入IP安全策略的名称如"屏蔽135端口"，再次单击"下一步"按钮，保持默认参数设置不变，直至完成位置，这样就创建出来了一个"屏蔽135端口"的安全策略，单击"确定"按钮返回。
- 2、设置IP筛选器
鼠标右击"IP安全策略"，选择"管理IP筛选器和筛选器操作"，进入到相应得对话框中，在"管理IP筛选器列表"页面中，点击"添加"按钮，在弹出的"IP筛选器列表"中输入名称"屏蔽135端口"，单击"添加"按钮，再点击"下一步"按钮。在目标地址中选择"我的IP地址"，点击"下一步"按钮，在协议中选择"TCP"（一般选择此项，根据具体的端口设定，如关闭ICMP协议时，这里选择ICMP），如图3所示，点击"下一步"按钮，在设置IP协议端

口中选择从任意端口到此端口，在此端口中输入135，点击"下一步"按钮，即可完成屏蔽135端口的设置，单击"确定"按钮返回。其他端口的设置与此类似。

3、筛选器操作 还是在"管理IP筛选器和筛选器操作"对话框，进入到"管理筛选器操作"页面，点击"添加"按钮后，再单击"下一步"按钮，在名称中输入"拒绝"，点击"下一步"按钮。在筛选器操作中选择"阻止"项，点击"下一步"按钮，这样在管理筛选器操作中就会增加"拒绝"一项了。单击"关闭"按钮返回到"本地安全设置"对话框中。

在"本地安全设置"对话框中双击左侧窗口中的"IP安全策略在本地计算机"，我们可以看到右侧窗口中会出现"屏蔽135端口"字样，用鼠标右击这个新建的IP安全策略"屏蔽135端口"，选择"属性".在规则中选择"添加"，点击"下一步"按钮，选择"此规则不指定隧道"，接着点击"下一步"按钮，在选择网络类型中选择"所有网络连接"，点击"下一步"按钮，在IP筛选器列表中选择"屏蔽135端口。点击"下一步"按钮，在出现的窗口中选中前面操作中添加的"拒绝"，单击"下一步"按钮，这样就将筛选器加入到了名为"屏蔽135端口"的IP安全策略中了，单击"确定"按钮返回。

4、指派 完成了"屏蔽135端口"的IP安全策略的建立，但是在未被指派之前，它并不会起作用。用鼠标右击"屏蔽135端口"，选择"指派"后，IP安全策略就生效了。同样的方法还可以关闭其他的无用端口，这样我们就亲手创建了一个安全的网络防火墙。

100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com