

浅谈IP安全策略：防范被Ping与封闭端口 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/250/2021_2022__E6_B5_85_E8_B0_88IP_E5_AE_c101_250966.htm 随着学校校园网越来越多人使用，用户对网络知识认知的提高，很多人在网上下载一些黑客工具或者用Ping命令，进行扫描端口、IP寻找肉机，带来很坏的影响。

Ping命令它可以向你提供的地址发送一个小的数据包，然后侦听这台机器是否有“回答”。查找现在哪些机器在网络上活动。使用Ping入侵即是ICMP入侵，原理是通过Ping在一个时段内连续向计算机发出大量请求使得计算机的CPU占用率居高不下达到100%而系统死机甚至崩溃。基于此，写这篇IP安全策略防Ping文章以保障自己的系统安全。

其实防Ping安装和设置防火墙也可以解决，但防火墙并不是每一台电脑都会去装，要考虑资源占用还有设置技巧。如果你安装了防火墙但没有去修改、添加IP规则那一样没用。有些配置不是很高为免再给防火墙占用资源用手工在自己系统中设置安全策略是一个上上的办法。下面就写下具体创建过程：

：（一）创建IP安全策略 1、依次单击“开始 控制面板 管理工具 本地安全策略”，打开“本地安全设置”，右击该对话框左侧的“IP安全策略，在本地计算机”选项，执行“创建IP安全策略”命令。（之间有些简单的点击下一步之类的过程省略不写） 2、在出现的“默认响应规则身份验证方法”对话框中我们选中“此字符串用来保护密钥交换（预共享密钥）”选项，然后在下面的文字框中任意键入一段字符串。（如“禁止Ping”） 3、完成了IP安全策略的创建工作后在“IP筛选器列表”窗口中单击“添加”按钮，此时将会

弹出“IP筛选器向导”窗口，我们单击“下一步”，此时将会弹出“IP通信源”页面，在该页面中设置“源地址”为“我的IP地址”：“目标地址”为“任何IP地址”，任何IP地址的计算机都不能Ping你的机器。在“筛选器属性”中可封闭端口。比如封闭TCP协议的135端口：在“选择协议类型”的下拉列表中选择“TCP”，然后在“到此端口”下的文本框中输入“135”，点击“确定”按钮，这样就添加了一个屏蔽TCP 135（RPC）端口的筛选器，它可以防止外界通过135端口连上你的电脑。重复可封闭TCP UDP等自己认为需要封闭的端口。这里不一一写出。

4、依次单击“下一步”“完成”，此时，你将会在“IP筛选器列表”看到刚刚创建的筛选器，将其选中后单击“下一步”，我们在出现的“筛选器操作”页面中设置筛选器操作为“需要安全”选项。（二）指派IP安全策略 安全策略创建完毕后并不能马上生效，我们还需通过“指派”功能令其发挥作用。方法是：在“控制台根节点”中右击“新的IP安全策略”项，然后在弹出的右键菜单中执行“指派”命令，即可启用该策略。至此，这台主机已经具备了拒绝其他任何机器Ping自己IP地址的功能，不过在本地仍然能够Ping通自己。经过这样的设置之后，所有用户（包括管理员）都不能在其他机器上对此服务器进行Ping操作。从此你再也不用担心被Ping威胁。如果再把一些黑客工具、木马常探寻的端口封闭那你的系统就更加固若金汤了。

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