

打造坚实Vista防火墙防范木马病毒入侵 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/259/2021\\_2022\\_\\_E6\\_89\\_93\\_E9\\_80\\_A0\\_E5\\_9D\\_9A\\_E5\\_c100\\_259028.htm](https://www.100test.com/kao_ti2020/259/2021_2022__E6_89_93_E9_80_A0_E5_9D_9A_E5_c100_259028.htm) 引言：Windows vista防火墙在很多情况下都被网友“误解”了，以为它只存在“开启”或“关闭”的功能。事实并非如此，只是它的一些“高级功能”还没有被我们发现，一旦我们将这些“高级功能”挖掘并应用，那么您的系统将会处在一个安全又高效的工作环境中。熟悉操作系统的用户都知道，很多病毒都是通过端口来攻击系统的，比如“大名鼎鼎”的“冲击波”病毒，它就是通过“svchost.exe”进程打开的135端口感染并攻击系统的。现在摆在大家眼前的问题是，很多病毒（如熊猫烧香、威金等）都是通过上述的端口传播病毒。此外，还有很多端口都会给系统带来潜在的危险，最典型的莫过于3389端口，它甚至已经演变成为了“肉鸡的”代名词。如果我们直接将这些端口屏蔽，虽然可以减少病毒攻击的几率，但是随之而来的问题是，局域网内的其他机器无法访问你的计算机。小知识：Windows系统有很多端口，每个端口对应着有它自己的功用。这些端口在拥有一个功用的同时，也将系统的安全问题暴露了出来。最典型的莫过于3389端口，它是远程桌面使用的端口，但是现在已经演变成为“肉鸡的”代名词。针对上述的情况，有朋友说，我们可以通过建立端口规则来解决问题。可我想问了？那么多的端口，难道你一个一个个都建立么？对此，笔者认为还是建立一个出入规则，将一些敏感的端口屏蔽，这样做才比较合理。在运行里输入“secpol.msc”，回车后打开“本地安全策略”，在窗中左侧依次打开“

安全设置” “高级安全 Windows 防火墙-本地组策略对象”  
“入站规则”。接下来，我们就是要在这一里“做文章”，  
让Windows Vista系统防火墙做到更好，更强。右键单击“入  
站规则”，在弹出的菜单中选择“新规则”，接着在弹出的  
“规则向导”中点选“端口”，然后单击“下一步”按钮。  
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](http://www.100test.com)