Win7到底能不能“ 裸奔 ”？计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Win7_E5_88_B0_E5_BA_95_c98_644927.htm Windows 7（以下简称Win 7）自发布以来，其诸多方面的改进一直被人们所关注，而在重要的安全防护方面，更是有“ 牛人 ”豪言：用Win 7完全不需要安装杀软，“ 裸奔 ”即可“ 畅游 ”互联网。“ 牛人 ”出此豪言，相信并非毫无依据，那么Win 7的安全防护到底如何？是否真如“ 牛人 ”所言，使用Win 7可以“ 裸奔 ”呢？ Win 7的安全防护系统，主要由一套完整的防护体系构成，包括内外兼修的防火墙、Windows Defender（恶意程序扫描工具）、IE 8、用户账号控制、数据执行保护等。并且它们并非各自为营，而是在“ 操作中心 ”的统一调度下，相互配合而形成对系统安全的防护。 安全防范第一关系统防火墙 在Windows XP（以下简称Win XP）时代，很多朋友都将它的防火墙比做，因为它只能对入站连接进行筛选，对具有反弹端口的木马来说，很容易穿透它，防护效果差强人意。甚至在安装一些杀软的时候，亦会提示关闭系统防火墙，可见其功能之羸弱。而在Win 7中，除了原有的“ Windows防火墙 ”，还新增了一个“ 高级安全Windows防火墙 ”。为了便于叙述，在这里，我们将“ 高级安全Windows防火墙 ”简称为“ 高级防火墙 ”。 Windows防火墙提供初级防护 Win 7并没有摒弃传统的“ Windows防火墙 ”，但与Win XP相比，多出了对专用网络和公用网络的控制（请参考高级防火墙部分）。默认情况下，Windows防火墙允许所有出站连接，同时阻止所有入站连接。要允许某一程序能进行入站连接，只要勾选它就行了。

这一设置虽然简单，但对筛选入站连接而言却十分有效，因为它是在阻止所有入站连接的大前提下仅为用户所需要的少量程序“ 开绿灯 ”，控制权掌握在用户自己手中。另外，如果某一程序尚处于阻止状态中，那么在程序运行时，Windows防火墙会自动弹出对话窗口，提示用户采取允许或拒绝的操作，从而避免影响正常工作。 因此，Windows防火墙在阻止入站连接上既有效又方便。一般适合于对安全要求不太高的环境，主要针对普通用户群体。 打开控制面板，单击“ Windows防火墙→允许程序或功能通过Windows防火墙 ”，即可打开设置界面。在默认状态下，供我们选择的项都处于灰色状态（不可用），必须单击“ 更改设置 ”才能对下面的选项进行修改。而这其实是一次权限提升的过程，因为在单击它之前是无权限修改设置的，单击时会弹出用户账号控制对话框，此时必须单击“ 是 ”才能更改，否则无法进行。估计大家都遇到过杀毒软件、防火墙被恶意程序关闭的情况，而使用用户账号控制其实就是一道屏障，如果用户不主动提升权限，是无法更改的，恶意软件也不行。 同时为了简化操作，用户账号控制也分为了四个级别。在最高的第一级状态下，更改设置会弹出用户账号控制对话框；在第二、三级别（从上向下）时，不弹出对话框，但用户账号控制仍然起作用；在第四级时，可直接修改（不推荐使用）。 高级防火墙提供更多选择 关于Win 7的高级防火墙，目前主要的评价是效果不错但设置难度高。其实真正使用后会发现，它的设置完全符合人们的逻辑思维习惯，而且有向导的指引，非常容易上手。高级防火墙既可创建入站规则，又可创建出站规则，相比之下，高级防火墙适用于安全环境要求较高，有一

定系统基础知识的高级用户。 在开始菜单的“ 搜索程序和文件 ”或“ 运行 ”窗口中输入“ Wf.msc ”并回车即可打开高级防火墙的主界面。 基本配置得心应手 这里以阻止QQ游戏的运行为例。右击“ 出站规则 ”选择“ 新建规则 ”，向导就会自动运行。首先需要指定对某一程序或端口进行设置，也可以选择“ 预定义 ”和“ 自定义 ”进行设置，其中“ 预定义 ”设置罗列了主要的系统操作，而“ 自定义 ”设置则更为广泛，可以涵盖系统所有的操作。本例中我们选择“ 程序 ”并找到QQ游戏的执行程序“ QQGame.exe ”，接着设置安全级别，比如：完全阻止还是只允许安全连接。本例选择“ 阻止连接 ”，然后再选择规则应用于什么范围，比如：域环境、专用网络、公用网络，最后输入该规则的名称即可完成。默认状态下，该规则处于开启状态，这样QQ游戏就不能运行了。来源：考试大 不同环境不同配置 目前，网络应用已呈多元化态势，Internet网、局域网等混合并存，同一程序或端口，会需要不同的入站、出站配置。一方面，网络环境的设置是Win 7推出的一项快捷的安全措施，包括家庭网络、工作网络、公用网络等，用户可根据需要进行快速切换以享受不同的安全防护规则。另一方面，我们还可针对每一种网络环境选择不同的连接，比如Internet网、局域网等。这些措施保障了高级防火墙配置的灵活多变，能应对不同的工作环境。来源：考试大 小贴士：在高级防火墙配置里，家庭网络和工作网络统称“ 专用 ”网络。 规则共享效率更高 创建了一条规则之后，我们就可以根据实际情况随时启用、停用规则，而它的另一优势在于可将配置好的规则导出备案，重新安装系统后只要导入即可免去重新配置之苦，同时还可以直接导入到

其他电脑上，从而大大提高工作效率。对于企业用户而言，这无疑是非常实用的功能。来源：考试大 在微软操作系统史上，IE的安全性是最受争议的。而IE的工作环境也将它推上了病毒防范的前沿阵地因特网，病毒传播的主要媒介。而在Win 7中，IE8的改进也使它成为有效防范病毒的一道屏障。“ 火眼金睛 ”识别假冒网站 Microsoft SmartScreen 筛选器可谓给IE装上了孙大圣的“ 火眼金睛 ”，有了它，可以有效防止网络钓鱼攻击、联机欺诈和欺骗网站以及发布恶意软件的网站带来的威胁。如果遇到这类网站，整个网页背景、地址栏都将显示为醒目的红色，并给出明显的文字提示。此外，域名突出显示也可帮助我们识别恶意网站。 保护模式给系统穿上“ 铁布衫 ” 中毒，很多时候是在上网过程中不知不觉地“ 中招 ”的，而在IE8中启用“ 保护模式 ”和加载项管理，则可以有效防止恶意程序的下载，另外，InPrivate 筛选器、跨站点脚本 (XSS) 筛选器还可以有效防止个人信息外泄。可以说，IE8作为病毒防范的前沿阵地，不仅充分考虑了系统安全，还将其扩展到了个人隐私领域，可以说给系统穿上了“ 铁布衫 ”，形成了初步的防范屏障。 在Win XP系统中，用户分为“ 计算机管理员 ”和“ 受限用户 ”两种模式。管理员可以进行系统设置、修改等操作，但安全性低，除用户的错误的设置使系统安全性降低外，更严重的表现是恶意程序也会借用高权限对系统进行为所欲为的破坏。如果使用受限用户，安全性比较高，但又会因某些程序无法运行而影响工作效率。来源：www.100test.com 在Windows Vista系统中，这一功能得到了改进，推出了“ 用户账户 ”控制，并在Win 7中得到了继承。不论是系统管理员还是标准用户，系统都会对用户操

作进行监视，一旦涉及系统安全的操作，管理员用户必须单击弹出对话框中的“ 确定 ”以暂时提升权限才能让操作继续；而标准用户还必须输入管理员密码才能进行。不难看出，纵使以管理员身份登录，要使用最高权限也必须手动操作，这就避免了恶意程序利用管理员身份修改系统设置，使其胎死腹中、无法得逞。 统一管理 发挥最大效能 在Win 7中，上述安全防范措施都在安全中心的统一管理下“ 协同作战 ”。打开控制面板下的“ 操作中心 ”，可以看到一块与安全相关的管理窗口。包括上述系统自带的安全措施和第三方工具无一例外地纳入到它的管理之下。在操作中心，可以观察到它们的工作状态是否正常、是否需要升级到最新版本等，为用户提供了最直接、最方便的管理。来源：www.100test.com 除了上述安全措施，Win 7中还包括Windows Defender（恶意软件扫描工具）和数据执行保护 (DEP），只不过二者在Win XP中就已经存在。前者如其名，扫描恶意软件，进行系统的基本维护；后者是一种软、硬件结合的防毒措施，两者结合后将生成一种全新的恶意代码防御机制：将所有内存位置均标记为不可执行除非该位置已明确包含可执行代码。当有攻击程序企图在不可执行的内存位置中插入代码并执行代码时，这一行为将会被阻止。不难想象，除非得到了用户的允许，不明代码是很难执行的，这在很大程度上扼制了病毒等恶意软件的入侵。 总结：“ 裸奔 ”依然危险 杀毒软件仍不可少 这么多的安全防护措施使Win 7的“ 裸奔 ”成为了可能。不过要“ 裸奔 ”，还必须可以善用各种安全功能，良好的安全意识以及规范的上网行为。比如：通过改进的任务管理器监控程序，结束恶意进程，并可以手动删除；使用标准用户让系统

工作于高安全状态；使用软件控制策略、家长控制限制程序的运行等。总之，调用一切资源来保障系统安全。不过对普通用户而言，显然上述要求有些过高。来源：www.examda.com 如果只用Win 7的防火墙而放弃第三方防火墙并非不可取，但杀毒软件绝对不可放弃，微软自己推出杀毒软件Morro就是最好的证明。而且Win 7对于主流杀毒软件的兼容性已经很好，因此董师傅建议大家，安装Win 7，“裸奔”仍不可取，杀毒软件依旧重要。 编辑特别推荐: 2009年9月全国计算机等级考试真题及答案 2009年9月全国计算机等级考试成绩查询 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