Windows防火墙探究 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/234/2021_2022_Windows_E9_98_B2_c100_234925.htm 如果回到过去的计算时代，没有人会考虑在单独的计算机上安装防火墙。谁需要这么做呢?很少有人听说过 Internet，TCP/IP 并不存在，LAN 协议不会在您的房子或校园上方传送。重要的数据都保存在大型机或文件服务器 人们保留在他们台式计算机上的信息很少会是关键性的，计算机自身的重量也一定程度上确保了相当的物理安全性。如果存在到 Internet 的连接，那么中间很可能有一些协议转换器，在网络边缘还可能有数据包筛选路由器(即“ 防火墙 ”)，而且很可能配置了太多的规则和异常处理。 现代的计算环境和这样的过去年代差别很大。每个设备都连接到 Internet(而且现在都用 TCP/IP 通信)，并且便携式设备是当前的标准。您的雇主很可能给您配了一台便携式计算机，这并不是因为他们关心您，而是因为他们希望您多做点贡献 他们非常希望您一旦有了五分钟的空闲，就可以随时随地通过 Wi-Fi 连接工作。便携式计算机也许比台式计算机昂贵，但是通过生产力的提高，这笔投资肯定得到了回报。您看，便携性是如此诱人 无论是对您还是对您的对手都是如此。 回想一下：在您的便携式计算机开机并连接到某个网络的总时间里，有多大比例是连接到您公司的网络?如果您的情况和我类似，也许最多是百分之二十。也就是说，只有百分之二十的时间里，我的便携式计算机安全地处在 Microsoft 的公司网络之内，受到网络外围防护的保护，以免遭到外部攻击。但是在百分之八十的时间里，我的便携式计算机因各种实际需要而

直接连接到 Internet，这会怎么样?(而且，我相当频繁地连接到世界上最危险的网络：计算机安全会议所在旅馆的 LAN!) 当我在那些场合连接到公司网络时，该环境内的其他计算机又会给我带来什么样的威胁? 安全控制不断发展以应对威胁，但有时候远远落在后面。病毒曾经是客户端的问题，原因是人们相互交换软盘，所以防病毒程序首先出现在客户端。此后，随着电子邮件得到广泛使用以及恶意软件逐渐演变为依靠电子邮件传播的蠕虫，反恶意软件的程序开始发展并出现在电子邮件网关上。随着 Web 的兴起，恶意软件逐渐演变为木马，反恶意软件工具随之出现在 Internet 访问代理服务器上。这是一个广为了解的发展过程，没有人对此有异议。 现在让我们把同样的逻辑用到防火墙上。虽然您网络边缘的防火墙足以抵御原先的威胁，但现在的威胁已不同以往，它们更加复杂，更加普遍。更不用说现在的设备和工作方式都与过去大相径庭。许多计算机在本地保存敏感的信息，而且在大量的时间里它们都处在公司网络之外(也就是说，在防护边缘之外)。因此，防火墙必须演化成单个客户端的保护机制。没错：客户端防火墙不再是可有可无的。为了在公司网络和 Internet 中保护您的计算机，客户端防火墙是必需的。 客户端防火墙和安全性表演 许多人没有意识到最初发布的 Windows#8482. 防火墙中的原因。(稍后我将进一步探讨有关 Windows Vista 中的出站控制。) Windows Vista 中有哪些新增功能? Windows 筛选平台作为新网络堆栈的一部分，是 Windows Vista 防火墙的根基。与 Windows XP 类似，Windows Vista 在默认情况下阻止入站通信。根据您的计算机运行的配置文件的不同，有可能存在网络服务的默认异常情况(稍后我

将讨论配置文件)。如果愿意，您可以编写允许入站连接的规则。仍然与 Windows XP 类似，Windows Vista 在默认情况下允许来自所有交互式进程的出站通信，但对参与服务限制的服务采取出站通信限制。同样，如果愿意，您可以编写阻止额外出站连接的规则。 Windows XP 和 Windows Vista 之间的最大区别是新的高级安全界面和对配置及规则的完全组策略支持(请参阅图 1)。原有的“ 控制面板 ”用户界面依然存在，除了登录和 Internet 控制消息协议 (ICMP) 设置之外(现在位于新用户界面中)，它基本上没有变化。这个新的用户界面(高级安全 MMC 管理单元)提供了所有全新的功能和灵活性。netsh 命令有了新的环境，即 netsh advfirewall，通过它您可以编写添加和删除规则的脚本，设置和显示全局及逐个配置文件策略，以及显示防火墙的活动状态。对开发人员而言，用 FirewallAPI.dll 和 Netfw.h 可对防火墙的所有设置进行编程式控制。图 1 具有高级安全性的 Windows 防火墙 高级安全 MMC 是向导驱动的。创建规则时，您可以选择四种类型之一：程序、端口、预定义或者自定义。图 2 提供了相关说明。 在编写规则时可以引用许多元素，它们都适用于本地规则和通过组策略应用的规则。其中包括：Active Directory&reg. 用户和计算机帐户及组、源和目标 IP 地址、源和目标 TCP 及 UDP 端口、IP 协议号、程序和服务、接口类型(有线、无线和远程访问)以及 ICMP 类型和代码。 