

配置Windows2008系统的高级防火墙Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/623/2021_2022__E9_85_8D_E7_BD_AEWind_c100_623930.htm 微软的Windows Server 2003中防火墙的功能如此之简陋，让很多系统管理员将其视为鸡肋，它一直是一个简单的、仅支持入站防护、基于主机的状态防火墙。而随着Windows Server 2008的日渐向我们走近，其内置的防火墙功能得到了巨大的改进。下面让我们一起来看一下这个新的高级防火墙将如何帮助我们防护系统，以及如何使用管理控制台单元来配置它。为什么你应该使用这个Windows的基于主机的防火墙？今天许多公司正在使用外置安全硬件的方式来加固它们的网络。这意味着，它们使用防火墙和入侵保护系统在它们的网络周围建立起了一道铜墙铁壁，保护它们自然免受互联网上恶意攻击者的入侵。但是，如果一个攻击者能够攻破外围的防线，从而获得对内部网络的访问，将只有Windows认证安全来阻止他们来访问公司最有价值的资产-它们的数据。这是因为大多数IT人士没有使用基于主机的防火墙来加固他们的服务器的安全。为什么会出现这样的情况呢？因为多数IT人士认为，部署基于主机的防火墙所带来的麻烦要大于它们带来的价值。我希望在您读完这篇文章后，能够花一点时间来考虑Windows这个基于主机的防火墙。在Windows Server 2008中，这个基于主机的防火墙被内置在Windows中，已经被预先安装，与前面版本相比具有更多功能，而且更容易配置。它是加固一个关键的基础服务器的最好方法之一。具有高级安全性的Windows防火墙结合了主机防火墙和IPSec.与边界防火墙不同，具有高级安全

性的 Windows 防火墙在每台运行此版本 Windows 的计算机上运行，并对可能穿越边界网络或源于组织内部的网络攻击提供本地保护。它还提供计算机到计算机的连接安全，使您可以对通信要求身份验证和数据保护。那么，这个 Windows Server 高级防火墙可以为你做什么，你又该如何配置它？让我们继续看下去。新防火墙具备的功能及对你的帮助

这个 Windows Server 2008 中的内置防火墙现在“高级”了。这不仅仅是我说它高级，微软现在已经将其称为高级安全 Windows 防火墙（简称 WFAS）。以下是可以证明它这个新名字的新功能：

- 1、新的图形化界面。现在通过一个管理控制台单元来配置这个高级防火墙。
- 2、双向保护。对出站、进站通信进行过滤。
- 3、与 IPSEC 更好的配合。具有高级安全性的 Windows 防火墙将 Windows 防火墙功能和 Internet 协议安全（IPSec）集成到一个控制台中。使用这些高级选项可以按照环境所需的方式配置密钥交换、数据保护（完整性和加密）以及身份验证设置。
- 4、高级规则配置。你可以针对 Windows Server 上的各种对象创建防火墙规则，配置防火墙规则以确定阻止还是允许流量通过具有高级安全性的 Windows 防火墙。传入数据包到达计算机时，具有高级安全性的 Windows 防火墙检查该数据包，并确定它是否符合防火墙规则中指定的标准。如果数据包与规则中的标准匹配，则具有高级安全性的 Windows 防火墙执行规则中指定的操作，即阻止连接或允许连接。如果数据包与规则中的标准不匹配，则具有高级安全性的 Windows 防火墙丢弃该数据包，并在防火墙日志文件中创建条目（如果启用了日志记录）。对规则进行配置时，可以从各种标准中进行选择：例如应用程

序名称、系统服务名称、TCP端口、UDP端口、本地IP地址、远程IP地址、配置文件、接口类型（如网络适配器）、用户、用户组、计算机、计算机组、协议、ICMP类型等。规则中的标准添加在一起；添加的标准越多，具有高级安全性的Windows防火墙匹配传入流量就越精细。通过增加双向防护功能、一个更好的图形界面和高级的规则配置，这个高级安全Windows防火墙正在变得和传统的基于主机的防火墙一样强大，例如ZoneAlarm Pro等。我知道任何服务器管理员在使用一个基于主机的防火墙时首先想到的是：它是否会影响这个关键服务器基础应用的正常工作？然而对于任何安全措施这都是一个可能存在的问题，Windows 2008高级安全防火墙会自动的为添加到这个服务器的任何新角色自动配置新的规则。但是，如果你在服务器上运行一个非微软的应用程序，而且它需要入站网络连接的话，你将必须根据通信的类型来创建一个新的规则。通过使用这个高级防火墙，你可以更好的加固你的服务器以免遭攻击，让你的服务器不被利用去攻击别人，以及真正确定什么数据在进出你的服务器。下面让我们看一下如何来实现这些目的。了解配置Windows防火墙高级安全性的选择在以前Windows Server中，你可以在去配置你的网络适配器或从控制面板中来配置Windows防火墙。这个配置是非常简单的。对于Windows高级安全防火墙，大多数管理员可以或者从Windows服务器管理器配置它，或者从只有Windows高级安全防火墙MMC管理单元中配置它。我发现启动这个Windows高级安全防火墙的最简单最快速的方法是，在开始菜单的搜索框中键入‘防火墙’快速启动Windows 2008高级安全防火墙管理控制台的方法 另外，你

还可以用配置网络组件设置的命令行工具Netsh来配置Windows高级安全防火墙。使用netsh advfirewall可以创建脚本，以便自动同时为IPv4和IPv6流量配置一组具有高级安全性的Windows防火墙设置。还可以使用netsh advfirewall命令显示具有高级安全性的Windows防火墙的配置和状态。使用新的Windows高级安全防火墙MMC管理单元能配置什么？由于使用这个新的防火墙管理控制台你可以配置如此众多的功能，我不可能面面俱到的提到它们。如果你曾经看过Windows 2003内置防火墙的配置图形界面，你会迅速的发现在这个新的Windows高级安全防火墙中躲了如此众多的选项。下面让我选其中一些最常用的功能来介绍给大家。默认情况下，当你第一次进入Windows高级安全防火墙管理控制台的时候，你将看到Windows高级安全防火墙默认开启，并且阻挡不匹配入站规则的入站连接。此外，这个新的出站防火墙默认被关闭。你将注意的其他事情是，这个Windows高级安全防火墙还有多个配置文件供用户选择。在Windows 2008高级安全防火墙中提供的配置文件在这个Windows高级安全防火墙中有一个域配置文件、专用配置文件和公用配置文件。配置文件是一种分组设置的方法，如防火墙规则和连接安全规则，根据计算机连接的位置将其应用于该计算机。例如根据你的计算机是在企业局域网中还是在本地咖啡店中。在我看来，在我们讨论过的Windows 2008高级安全防火墙的所有改进中，意义最重大的改进当属更复杂的防火墙规则。看一下在Windows Server 2003防火墙增加一个例外的选项。Windows 2003 Server防火墙例外窗口再来对比一下Windows 2008 Server中的配置窗口。Windows 2008 Server高级防火墙例外设置窗

口 注意协议和端口标签只是这个多标签窗口中的一小部分。你还可以将规则应用到用户及计算机、程序和服务以及IP地址范围。通过这种复杂的防火墙规则配置，微软已经将Windows高级安全防火墙朝着微软的IAS Server发展。Windows高级安全防火墙所提供的默认规则的数量也是令人吃惊的。在Windows 2003 Server中，只有三个默认的例外规则。而Windows 2008高级安全防火墙提供了大约90个默认入站防火墙规则和至少40个默认外出规则。Windows 2008 Server高级防火墙默认入站规则 那么你如何使用这个新的Windows高级防火墙创建一个规则呢？让我们接下来看一下。如何创建一个定制的入站规则？假如说你已经在你的Windows 2008 Server上安装了Windows版的Apache网站服务器。如果你已经使用了Windows内置的IIS网站服务器，这个端口会自动会为你打开。但是，由于你现在使用一个来自第三方的网站服务器，而且你打开了入站防火墙，你必须手动的打开这个窗口。以下是步骤：识别你要屏蔽微软认证加入收藏！的协议-在我们的例子中，它是TCP/IP（与之对应的则是UDP/IP或ICMP）。识别源IP地址、源端口号、目的IP地址和目的端口。我们进行的Web通信是来自于任何IP地址和任何端口号并流向这个服务器80端口的数据通信。（注意，你可以为一个特定的程序创建一条规则，诸如这儿的apache HTTP服务器）。打开Windows高级安全防火墙管理控制台。增加规则-点击在Windows高级安全防火墙MMC中的新建规则按钮，开始启动新规则的向导。Windows 2008 Server高级防火墙管理控制台-新建规则按钮 为一个端口选择你想要创建的规则。配置协议及端口号-选择默认的TCP协议，并输入80作为端口，然

后点击下一步。选择默认的“允许连接”并点击下一步。选择默认的应用这条规则到所有配置文件，并点击下一步。给这个规则起一个名字，然后点击下一步。创建规则后的Windows 2008 Server高级防火墙管理控制台 经过我测试，当不启用这个规则的时候，我最近安装的Apache网站服务器不能正常工作。但是，创建了这个规则后，它可以正常工作了！结论：大有改进 值得一试 具有防火墙配置文件、复杂的规则设置和原先30倍数量的默认规则，还有本文中未提到很多高级安全功能，Windows 2008 Server高级安全防火墙的确名副其实，真正是一个微软所说的高级防火墙。我相信这个内置、免费、高级的基于主机的防火墙将确保Windows Server未来变得更加安全。但是，如果你不使用它，它不会对你有任何帮助。因此我希望你今天就来体验一下这个新的Windows高级防火墙。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