控制VPN的连接权限巧设Win8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_ti2020/643/2021_2022__E6_8E_A7_E5_88_B6VPN_E7_c100_643918.htm 为了尽可能地降低组网费用，同时不能影响移动办公的需求，某单位决定在局域网的文件服务器中安装配置VPN服务器，这样可以让单位可信任员工随时随地通过VPN网络连接，访问单位文件服务器中的重要数据内容，并且这种访问方式安全性也能得到保证，可谓一举两得!最近，单位有一系列很重要的文件存放在VPN服务器中，单位领导希望这些文件只能允许某个特定的员工通过VPN连接进行访问，其他任何员工都无权访问.面对这样的访问需求，我们该如何才能实现呢?其实，要实现上面的网络访问目的，我们可以有多种方法可供选用.不过，在安装了Windows Server 2008系统的VPN服务器中，我们可以巧妙地使用该系统内置的高级安全防火墙，来实现更加灵活地控制!实现思路 我们知道，只要在Windows Server 2008系统中安装、配置好了VPN服务器，那么Internet网络中的任意一台VPN客户端系统都能通过VPN服务器中的“ 1723 ”端口，来访问其中的数据内容了，很显然我们只要能够想办法对VPN服务器中的“ 1723 ”端口进行有效控制，就能实现仅让指定员工有权访问VPN服务器中的重要文件目的了。而Windows Server 2008系统恰好为我们提供了高级安全防火墙功能，通过该功能我们可以按照实际需要定义访问VPN服务器的入站规则、出站规则，并且这些规则允许我们对网络连接进行验证操作，这么一来我们就能很轻易地将VPN网络连接权限授予单位特定的可信任员工了.甚至，我们还能设置访问规则，仅让指

定的VPN客户端系统访问VPN服务器，确保VPN服务器中的重要数据信息安全。 控制进入 为了仅让使用指定帐号的用户可以正常访问VPN服务器中的重要数据内容，我们可以授权特定帐号名称进入VPN服务器，并通过Windows Server 2008系统中的“ 1723 ”端口来进行资源访问操作，下面就是具体的实现方法： 首先以系统管理员身份登录进入Windows Server 2008服务器系统，依次单击该系统桌面中的“ 开始 ”/“ 程序 ”/“ 管理工具 ”/“ 服务器管理器 ”命令，在弹出的服务器管理器窗口中依次点选“ 配置 ”/“ 高级安全防火墙 ”分支选项. 其次在目标分支选项下面单击“ 入站规则 ”子项，在对应“ 入站规则 ”子项的右侧“ 操作 ”列表区域中，单击“ 新规则 ”按钮，打开创建新的入站规则向导对话框. 当向导窗口询问我们要创建什么类型的规则时，我们必须选中这里的“ 端口 ”选项，以便让Windows Server 2008服务器系统对通过VPN连接端口的数据包进行身份验证操作.选中“ 端口 ”选项后，单击“ 下一步 ”按钮，打开所示的向导设置界面，再将该设置界面中的“ TCP ”协议选项选中，同时选中“ 特定本地端口 ”选项，然后在对应“ 特定本地端口 ”选项的文本框中输入VPN服务器缺省使用的“ 1723 ”端口. 继续单击“ 下一步 ”按钮，系统屏幕上会出现一个所示的向导设置界面，选中其中的“ 只允许安全连接 ”选项，同时将该选项下面的“ 要求加密连接 ”子项选中，以便让Windows Server 2008服务器系统对来访者进行身份验证操作. 当向导屏幕出现所示的设置窗口时，我们可以选中这里的“ 只允许来自下列用户的连接 ”选项，同时单击该选项旁边的“ 添加 ”按钮，从其后出现的帐号选择对话框中，将我们认为可以信任的目标用户帐号导入

添加进来.最后依照向导提示，为当前创建的新入站规则取一个合适的名称，如此一来日后我们只有使用在这里授权的用户帐号才能访问Windows Server 2008系统中的VPN服务器，而使用其他用户帐号尝试与VPN服务器建立连接时，Windows Server 2008系统中的高级安全防火墙就会自动对它们进行拦截，这样一来VPN服务器中的重要数据信息就不会被他人随意访问了。