计算机一级辅导:解析微软的远程安全访问控制计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/583/2021_2022__E8_AE_A1_E7_AE_97_E6_9C_BA_E4_c98_583448.htm 2009年下半年全国计算机等级考试你准备好了没?考计算机等级考试的朋友,2009年下半年全国计算机等级考试时间是2009年9月19日至23日。更多优质资料尽在百考试题论坛 百考试题在线题库 远程访问一直是个热门话题，人们需要能够随时随地通过任何设备登录网络获取信息。过去利用特定设备或者特定位置访问网络的时代已经过去了，特别是在企业内，人们希望在任何时候都能获取企业信息，可能使用笔记本、台式机、智能手机或者甚至MP3播放器来获取企业信息。 微软公司就正在为此付出努力，希望能够保证用户随时随地使用各种技术来进行安全远程访问。注意这里所说的是“ 安全远程访问 ”，实现远程访问并不困难，任何简单的NAT设备或者路由器都可以让用户对企业应用程序和设备进行远程访问。这里的安全远程访问就能够保护用户数据、企业服务器不受到安全威胁。 以下是几个重要的微软技术能够帮助用户实现对企业资源的安全远程访问： Windows Server 2008 NPS路由和远程访问VPN服务 Windows Server 2008终端服务网关 Microsoft ISA 2006和Forefront Threat Management Gateway (TMG，威胁管理网关) Intelligent Application Gateway 2007和Unified Access Gateway (UAG，统一访问网关) Windows Server 2008 NPS远程访问VPN服务 Windows Servers从Windows NT开始就加入了一个VPN服务器组件，这样用户就能对VPN使用PPTP(Point to Point Tunneling Protocol)。目前来说，大多数安全专家认为PPTP是

一种过时的VPN协议，而不应该用于生产网络中，因为该协议中存在很多安全问题。虽然现在有办法能够增强PPTP的安全级别(如双条件登录)，几乎很少使用PPTP。 在Windows 2000 Server中引进了L2TP/IPsec VPN协议，这也是Windows的重大进步，因为Ipsec渠道能够保证在证书转让发生之前保护信息的安全性。L2TP被用于创建虚拟网络，而Ipsec用于在虚拟网络连接创建隐私。L2TP/Ipsec的另一个主要优势在于，用户和设备认证能够同时进行，因为使用的是Ipsec。Windows 2000 Server中还允许用户使用更先进的EAP验证方法进行用户验证，这样证书和智能卡就能够用于用户身份验证。
Windows Server 2008在用户的VPN功能中加入了SSTP(Secure Socket Tunneling Protocol，安全套接字渠道协议)，这种协议的最大优点就是在SSL上运行，任何防火墙或者代理服务器能够运行外流的SSL。即使当客户位于防火墙或者代理服务器(甚至是基于代理服务器的防火墙，如ISA或者TMG防火墙)后也可以运行SSTP，SSTP属于Windows Server 2008 NPS路由和远程访问VPN服务的一部分，它能够利用L2TP/Ipsec使用的所有相同的用户验证协议。SSTP的唯一缺点在于，配置步骤需要非常严谨，如果没有严格按照顺序执行配置，管理将会变得非常复杂。可以说，对于Windows VPN管理员而言，SSTP仍然是一项巨大的工作。 Windows Server终端服务 在Windows Server的前几个版本中加入了路由和远程访问VPN解决方案，Windows Server同时还加入了终端服务组件(Terminal Services)，虽然在Windows NT的RTM版中没有此组件，不过在NT产品后序版本中也加入了该组件。终端服务随后在Windows Server 2000发布时被纳入了操作系统中。

在Windows Server 2003的终端服务中作出了些许改进，Windows Server 2008才让我们看到终端服务组件的重要改进。 在Windows Server 2008和即将发布的Windows Server 2008 R2中，我们将看到终端服务产品的重大改进。在基本的终端服务器中的终端服务，能够允许用户通过使用RDP协议连接到终端服务器。实际上，RDP协议已经大大改善，不过并不是RDP协议的改进让Windows Server 2008 Terminal Services产品如此引人注目。主要改进功能包括： Terminal Services Web Access(网络访问) Terminal Services Gateway(网关) Terminal Service RemoteApp(远程应用程序) 虽然windows Server以前的版本也有Terminal Services Web Access功能，而Windows Server 2008功能明显增强，因为2008版向网站加入了几项Terminal Services的新功能，另外，通过终端服务网站访问计算机和应用程序可以通过基于政策的访问规则来控制。 终端服务网关(TSG，Terminal Services Gateway)可以在世界的任何位置启用基于政策的终端服务访问，过去对终端服务的远程访问的主要问题在于，很多访问权不能允许对默认RDP端口(即TCP 3389)的对外访问。由于代理服务器通常只处理HTTP协议，当客户位于Web代理服务器后时，终端服务客户就不能通过网络到达终端服务。TSG是通过允许终端服务客户与RPC内的RDP建立渠道来解决这个问题的，然后将在HTTP内部建立渠道，并由SSL安全保护，因此只需要允许对TSG的对外SSL连接即可。当客户连接到TSG后，基于政策的访问规则就允许客户控制用户可以连接到的终端服务器或者应用程序。 在新的Windows Server 2008 Terminal Server中，我们能够选择发布终端服务器和/或应用程序。终端服务RemoteApp允许你通

过终端服务发布应用程序。因此，如果你想要你的用户访问Word或者PPT，你可以通过终端服务网关发布这些应用程序，这样用户就只能访问这些应用程序，而不是整个桌面。这对于安全而言是个很大的进步，因为使用的是最小权限原则，用户只能访问他们需要的内容，而不是其他多余的东西。这种访问是通过TSG来实现的，TSG能够启用对这些应用程序的基于政策的访问。 Internet安全和Acceleration Server 2006以及Forefront Threat Management Gateway (TMG) 前面讨论了包括Windows Server在内的平台服务，现在让我们看看微软公司为安全远程访问提供的其他网络安全应用程序，微软最早引入网络安全设备实在90年代后半期，他们发布了Proxy Server产品。这也使他们催生出第一个成熟的产品，Proxy Server 2.0，虽然Proxy Server 2.0是个很不错的代理服务器，虽然并没有设计为能够进行安全远程访问的网络安全设备。 微软公司在2000年底发布的Microsoft Internet Security和Acceleration Server (ISA) 2000是保证安全远程访问的网络边缘安全设备的先锋产品，该产品是一个多功能设备，能够进行安全出站访问，安全服务器发布和安全Web发布。另外，ISA 2000能够支持远程访问VPN用户以及站到站VPN。最重要的是，ISA2000被设计为边缘网络防火墙，这样用户就不再需要在ISA2000防火墙前面放置基于路由器的防火墙(第三层防火墙)。 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