网络技术辅导: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_ti2020/581/2021_2022__E7_BD_91_E7_BB_9C_E6_8A_80_E6_c98_581803.htm 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)。 然后，ISA2000防火墙是建立在威胁模式的，该威胁模式现在已经不存在了。这就是说，对于在上个世纪流行的威胁模式而言，任何防火墙外部的东西都是不可信的，任何防火墙内部的东西都是值得信赖。而新一代ISA防火墙，ISA2004防火墙就被设计为，没有网络是可信的，所有通过ISA防火墙进行的连接都需要对状态数据包和应用程序层进行检查。 ISA2004中，远程访问的安全性明显改善。对于Web发布(与Web代理服务器相反)而言，HTTP安全过滤主要用于

保护网站免受攻击，还添加了很多应用程序来保护对SMTP、DNS和其他应用程序服务器的攻击。最重要的是，远程访问和站对站VPN服务器组件现在可以让用户创建强大的基于用户/组访问控制，并采用与通过ISA防火墙的所有连接的数据包和应用程序层进行的相同的检查。 ISA2004被认为是微软公司防火墙产品中第一个可以供企业使用的边缘网络防火墙，与Check Point、ASA以及Netscreen一样。 两年后发布了ISA2006，其中包含了所有2004ISA防火墙中的所有远程访问安全功能，另外还包含对远程访问安全功能的几个改进功能：支持Kerberos Constrained Delegation (KCD)，这样就可以发布要求用户在防火墙使用双条件证书验证的网站。 对其基于窗体验证功能的一些改进，这样用户就可以在获准访问网站前使用更加灵活的形式通过防火墙的验证。 扩大对一些新的双因素验证方法的支持，例如RADIUS一次性密码验证。 针对发布网站的LDAP服务器验证，这样当防火墙不是域成员时可以使用Active Directory存储区。 Web Farm Load Balancing可以使ISA2006管理员避免承受价格高昂的外部硬件负载均衡器和在ISA防火墙后发布大量Web服务器 ISA2006也可以配置为启用对所有Windows Server 2008 Terminal Services功能的安全远程访问，允许对远程服务访问的另一层保护。 Forefront Threat Management Gateway (TMG，威胁管理网关)是新版本的ISA防火墙，TMG保护前一个版本防护墙的所有安全远程访问技术，但是对于出站访问安全，还加入了恶意软件保护和独特的功能强大的IDS入侵检测功能。此外，TMG还能启用web内容过滤功能，这也是ISA防火墙管理员期盼很久的功能。 Intelligent Application Gateway 2007和UAG Intelligent

Application Gateway 2007 (IAG 2007)主要是针对企业的产品，能够帮助企业实现远程访问连接的最高级别安全水平，与ISA或者TMG防火墙相比，IAG 2007 SSL VPN网关是一种单一目的的装置：提供对网络设备入站连接的远程访问网关。ISA和TMG防火墙可以提供与目前市场上防火墙相同级别或者更高级别的网络设备入站连接安全，IAG2007能够为web和非web服务的入站连接提供最高级别的安全性。 IAG包括一些软件模块，被称为应用程序优化(Application Optimizers)，能够为对web服务的远程访问提供非常高的安全保护。应用程序优化能够使IAG为其发布的web服务执行深层次的应用程序层检查。IAG的深层应用程序层检查同时进行正面和反面的逻辑过滤，正面逻辑过滤使IAG只允许对发布的web服务进行可信的通信，而反面过滤能够阻止不可信的连接。 IAG 2007 SSL VPN能够支持以下四种连接： 反向Web代理服务，IAG可以通过对Web服务进行远程连接部署智能应用程序来充当高安全性的反向web代理。 端口转发器(Port Forwarder)，对于需要使用简单协议(使用单个端口)非web应用程序的远程访问，IAG端口转发器允许客户端使用该转发器通过SSL VPN渠道连接到网络应用程序。 套接字转发器(Socket Forwarder)，对于需要多个主要或者次要连接(如Outlook MAPI/RPC)的对复杂应用程序的远程访问，远程访问客户端可以使用IAG套接字转发器，所有通过套接字转发器通信的协议都受到SSL的保护。 网络链接器，网络链接器允许通过SSL VPN连接的完全网络层VPN访问，这对于需要对网络进行远程控制的管理员而言非常有用。 除了SSL VPN网关功能外，IAG 2007还允许PPTP和L2TP/Ipsec远程访问VPN客户端访问，这可以让你

使用IAG 2007作为中央远程访问网关，而不需要将几种设备或者各种类型的设备间网络的远程访问连接的管理和检测工作进行分离。 新版本的IAG被称为UAG(Unified Access Gateway，统一接入网关)，将继续加强IAG的应用程序层安全性，并将添加更多的安全远程访问功能。其中最有趣的功能就是，能够支持微软的新的Direct Access远程连接功能，这使位于世界各地的用户能够完全连接到企业网络，包括域连接等。 使用Direct Access的主要障碍在于它对Ipv6的依赖，虽然Ipv6有很多优点，但是大多数网络的架构并不支持Ipv6，另外，IPv6并没有得到大家的普遍认同，所以将其部署在网络上将是很危险的事情，因为大多数网络管理员将无法理解Ipv6生成的通信。 为了缓解Direct Access和Ipv6带来的连接性问题和安全挑战，UAG部署了NAT-PT(Network Address Translation Protocol Translation)，它能够允许本地Ipv6主机和应用程序与本地Ipv4主机和应用程序的通信，反之亦然。该功能可以为即将发布的Windows 7和Windows Server2008 R2网络部署Direct Access解决方案变得更加简单更安全。 总结 本文中我们讨论了现有微软网络中的安全远程访问功能，有些功能在早期windows NT版本中就已经存在，而有些功能只有在部署Windows 7和Windows Server 2008 R2后才能使用。这些功能都有自己的优点和缺点，并且提供不同级别的安全性，不同类型的远程访问。希望大家在阅读完本文后，能够更好的理解远程访问功能并能够根据自己所需选择适合的远程访问设备。 特别推荐： 2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总

2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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