玩转VPN虚拟专用网给网络架设隧道 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E7_8E_A9_E8_BD_ACVPN_E8_c101_142873.htm 最近两年虚拟专网VPN技术被业界吵得火热，很多企业都通过VPN实现了远程拨入以及分支连接的功能，一方面方便了企业员工顺利开展业务，另一方面节约了大量专线铺设的经费。当然与之而来的是很多厂商开发了专业的硬件VPN产品，那么我们是否可以通过软件设置来替代这些硬件产品呢？答案是肯定的，今天笔者就为各位全盘呈现软件VPN建立的方法。 一般来说不通过硬件VPN产品建立虚拟专网的方法主要有两种，一种是在Windows server服务器（包括2000 server或2003 server），另外一种则是使用路由器或三层交换机提供VPN接入服务。 从应用场合上讲前者主要是在方便原远程拨号，从家中连接企业内部网的环境，这样员工就可以在家中通过VPN拨号连接企业的VPN接入服务器，从而实现远程办公的目的了。而使用路由器或三层交换机提供VPN接入服务则更适合于互连企业多个分支机构到本部的场合，这样可以保证分支机构的所有员工计算机可以正常访问本部的内部计算机和服务器。 下面笔者就依次介绍通过服务器和路由交换设备建立VPN接入服务的办法，各位读者可以根据自己企业的实际情况去选择。 一、Windows2000/2003架设 通过操作系统建立虚拟专线网络主要分两大步，第一是在服务器上进行设置，开启路由和远程访问服务并设置拨入帐户的权限；第二是在客户端建立一个VPN拨号连接，通过网络连接到VPN服务器上。 1、VPN服务器的建立 一般来说我们可以使用windows 2000

或windos 2003操作系统来充当VPN服务器。 首先通过桌面“开始->所有程序->管理工具->路由和远程访问”来启动路由和远程访问组件。打开“路由和远程访问”组件后我们在服务器名称上点右键选择“配置并启用路由和远程访问”（如图1）。图1 之后会启动路由和远程访问服务器安装向导，为了方便企业设置我们选择最下方的“自定义配置”，然后点“下一步”按钮。接下来选择想在此服务器上启用的服务，我们将“VPN访问”和“请求拨号连接（由分支办公室路由使用）”两项打勾即可（如图2）。图2 所有设置完毕后我们结束路由和远程访问服务器安装向导工作，点“完成”按钮的同时将会开启路由和远程访问服务。 现在我们还需要就几个参数进行深入设置，在“路由和远程访问”本地服务上点鼠标右键选择“属性”。找到IP标签设置一下用于分配给远程拨入计算机的IP地址（如图3）。图3 仅仅如此还不够，远程计算机在拨入VPN服务时会出现权限不足的问题，因此我们还需要设置拨入权限。方法是在“计算机管理->用户管理”找到你容许远程接入的帐户，然后打开属性页面，选择“拨入”标签，将远程访问权限（拨入或VPN）处设置为“容许访问”。当然在“拨入”标签下有很多设置提供给我们，各位根据企业实际调整参数即可。确定完毕后我们才能在远程计算机上使用此帐户顺利连接VPN服务器（如图4）。图4 2、VPN客户端的连接 接下来就要设置普通员工计算机的VPN连接了，我们只需要按照传统访问建立一个本地拨号连接即可。当然VPN顺利接入是建立在我们的计算机已经通过ADSL或其他方式连接到internet网的情况下进行的。 打开客户机系统中的本地连接窗口，然后新建一个连接。在新建连接向导

中选择“ 连接到我的工作场所的网络 ”；接下来的网络连接选择“ 虚拟专用网络连接 ”，点“ 下一步 ”按钮继续（如图5），再设置一个连接名称，这里笔者输入softer。图5 由于我们当前已经连接到了internet，所以在“ 公用网络 ”设置处选择“ 不拨初始连接 ”。当然如果你希望用VPN拨号触发Internet拨号的话可以设置“ 自动拨此初始连接 ”。 建立完毕后会在桌面创建一个VPN拨号连接，我们在用户名处输入拨入帐户，密码输入帐户对应的密码，在服务器地址处输入VPN服务器的IP地址，然后点“ 连接 ”按钮即可。如果网络连接和路由信息正确的话将自动连接。之后我们就可以顺利打开网上邻居或者通过IP访问企业内部的计算机和服务器了（如图6）。图6 至此我们就完成了通过操作系统建立VPN服务器并在客户端顺利接入的工作，员工可以在家中或者在外出差时顺利访问企业内网资源了。 二、路由器配置VPN虚拟专网 不过有的时候企业在不同地方开设了分支机构，而要保证这些分支机构之间有如一个内网一样，这就需要虚拟专网VPN了。不过不同于上面提到的单个客户机和企业内网的VPN连接，分支机构互连是建立在网络和网络直接VPN连接基础上的，仅仅依靠一台windows系统建立的VPN服务器是绝对不能满足应用的，这时就需要在两头的路由交换设备上设置VPN信息进行连接了（如图7）。图7 1、总部路由器的设置 总部路由器是VPN建立的核心，大部分加密验证工作都放在此。 （1）创建ISAKMP策略及添加加密验证信息：crypto isakmp policy 1 encryption des hash sha authentication pro-sharegroup 1lifetime 28800 crypto isakmp identity addresscrypto isakmp key cisco123 address 10.0.0.2 crypto ipsec

transform-set bjset esp-des esp-md5-hmac crypto map bjmap 1 ipsec-isakmp （2）设置对端路由信息：set peer 10.0.0.2set transform-set bjsetmatch address 101int fa0/0ip address 172.16.1.1 255.255.255.0 （3）设置外网接口及加密图：int s0/0ip address 10.0.0.1 255.255.255.0no ip mroute-cacheno fair-queueclockrate 64000crypto map bjmap （4）应用加密信息：access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255access-list 101 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 2、分支路由器的设置 分支路由器上只需要按照主路由器参数并结合自己网络IP地址等信息即可。具体步骤也是上面的四步，依次为创建ISAKMP策略及添加加密验证信息，设置对端路由信息，设置外网接口及加密图，应用加密信息。设置完毕后两台路由器就完成了连接工作，两地员工可以像访问同一个内网资源一样访问对方服务和资源了。 三、总结 虚拟专网VPN帮助我们更好的应用企业服务，开展企业业务，更关键的是还可以省去大量的不必要网络带宽租用开支。不过在实施VPN方案时一定要根据自己的实际环境决定，尽量采用通过windows服务器建立VPN服务的方法，毕竟路由器的设置比较麻烦，密钥没设置好就无法顺利连接，排查起故障也很棘手。 