基于 Windows 2000 的远程访问 VPN 实现

The Implementation of Remote Access VPN on Windows 2000

江 魁 黄云森（深圳市深圳大学网络中心 518060）

摘要：本文以一个校园网中的远程访问应用为例，在简单介绍 VPN 的基础上分析了 Windows 2000 下远程访问 VPN 的特点，阐述了在 Windows 2000 下实现远程访问 VPN 的步骤。实践证明这是一个简洁高效的远程访问解决方案。

关键词：远程访问 Windows 2000 VPN

1 引言

我校网络从 1988 年开始建设，经过多次扩建和升级，目前已成为拥有超过一万个信息点的大型园区网。一直以来，我校通过 Cisco 2511 作为拨号远程访问服务器为教师远程办公和校外用户提供远程访问服务，用户从校外直接拨号到远程访问服务器来访问校园网络内部资源[1]。这种方式虽然解决了用户从校外访问校内特定资源（如图书馆数据库，内部公文系统）的问题。但存在以下问题与不足：(1)教师出差在异地时需要通过长途拨入到校内拨号服务器，长途费用开销较大；(2)由于校内提供拨入的电话号码不是类似于电信 163 之类的特服号，用户本地拨入时以普通市话计费，与拨号到 ISP 的特定号码相比费用较高；(3)校外用户与内部网中的计算机进行数据传输时，无法保证通信的安全性；(4)由于拨号服务器采用 MODEM 作为接入设备，提供的接入速率有限，一般不超过 56K。由于不少教师在家中已经采用 ADSL 等宽带上网，因此从家中访问校内资源时拨号服务器成为制约网络访问的瓶颈。经过仔细的分析和比较，我们最终采用了基于 Windows 2000 的虚拟专用网（VPN）取代了 Cisco 2511 提供远程访问服务，成功地解决了以上问题。

2 VPN 简介

虚拟专用网（VPN）是部署于公共网络（Internet、帧中继、ATM 等）上的一种网络，用于在远程用户、单位分支机构、合作单位与单位的内部网建立一条安全的隧道，保证数据的安全传输。VPN 是在现有的公共网络基础设施上实现的，无须花费昂贵的专线连接费用和长途电话费用，并且使用与专用网络相同的安全性、管理以及服务质量策略，因此 VPN 可以看作是对单位内部网的扩展。使用 VPN 的优点在于降低连接的成本，同时将内部网络的连续性安全有效地扩展到远程移动用户、家庭用户、远程办公室以及合作单位。

当前 VPN 的连接类型主要有远程访问连接和路由器对路由器连接两种。远程访问连接使远程移动用户和家庭用户可以通过 Internet 对单位的内部网络进行远程访问。路由器对路由器的 VPN 连接主要用于合作单位通过 Internet 与单位自身连接起来。

VPN 的实现原理主要是隧道技术，利用隧道在新的数据包里封装原始数据包。隧道端点的地址在外部的新包头里提供，这个包头称为封装头，这样就能保证封装后的数据包能够通过隧道，而最后的目的地址装在原始的数据包头里。当数据包到达隧道的终点时，将封装头剥去，原始数据包头被用来将数据包路由到最终目的地。当前常用的隧道协议主要有点到点隧道协议 PPTP、第二层隧道协议 L2TP、网络层隧道协议 IPSec 三种[2]。

3 Windows 2000 下的 VPN

VPN 的实现可以采用硬件和软件两种方式。硬件方式可以是具有 VPN 连接功能的路由器、防火墙，甚至是各厂商设计的专用 VPN 交换机，如思科的 VPN Concentrator 3000，北电的 Contivity 等。这种方式缺点是价格高，使用复杂，若仅仅是提供远程访问服务则没有必要用这类设备。因此，我们最终选用了基于 Windows 2000 的软件 VPN 连接方式。

Windows 2000 下的 VPN 主要采用 PPTP 和基于 IPSec 的 L2TP 两种隧道协议。PPTP 利用点对点协议（PPP）用户身份验证和 Microsoft 点对点加密（MPPE）来封装和加密 IP、IPX 、NetBEUI 通信，PPTP 只加密 VPN 隧道两端之间传输的数据。L2TP 利用 PPP 对 IP、IPX 、NetBEUI 通信进行封装和用户身份验证，与 PPTP 不同的是 L2TP 不依靠 Microsoft 点对点加密协议对 PPP 数据报文进行加密，而通过 IPSec 来提供加密服务。L2TP 先通过 IPSec 使用基于证书的计算机身份验证来创建安全的和加密的通道，然后基于 PPP 的用户身份验证来创建 L2TP 隧道。基于 IPSec 的 L2TP 为每个数据包都提供数据完整性和数据身份验证。但是这种方式需要使用公钥基本结构（PKI）来分配计算机证书，且只被 Windows 2000 VPN 客户端支持，Windows 95 /98、Windows NT 4.0 都不支持 L2TP

只支持 PPTP。考虑到校外用户使用的操作系统的多样性，因此我们选用了 PPTP 作为 Windows 2000 采用的隧道协议。

4 实现步骤

4.1 服务端

准备作为 VPN 服务器的 Windows 2000 机器应该同时有到 Internet 的连接和到校园内部网的连接，我们在该机器上安装了两块网卡，其中一块设定一个电信 IP 地址通过百兆连接到 Internet，另一块设定一个校内私有 IP 地址通过百兆连接到校园内部网络。这样该机器既能与 Internet 上的各个主机进行通信，同时也能与校园内部网中的各个主机正常通信。随后启用 Windows 2000 下的 VPN 服务，步骤如下：

依次单击开始、程序、管理工具和路由和远程访问，打开控制台。

右键单击服务器，单击“配置并启用路由和远程访问”，启动向导，单击“虚拟专用网络 (VPN) 服务器”，然后单击下一步。

在“远程客户协议”中，验证远程访问 VPN 客户端所使用的所有数据协议都存在。必要时添加数据协议，然后单击下一步。

在 “Internet 连接”中，单击与连接到 Internet 的接口相对应的连接，然后单击下一步。

在“网络选择”中，将远程 VPN 客户指定到想让他们使用的网络，然后单击下一步。

如果 VPN 服务器要用 DHCP 来获取远程访问 VPN 客户端的 IP 地址，则在“IP 地址指定”中选择“自动”。如果为远程客户指定使用静态地址范围，选择“来自一个指定的地址范围”。这里我们单击“自动”，通过 DHCP 服务器来分配地址，这样做的一个好处是可以在分配 IP 地址的同时将 DNS 服务器、WINS 服务器等相关参数也分配给客户，值得注意的是如果分配出去的 IP 地址范围不属于连接到内部网络的网卡所在的网段，必须在内部网络的三层设备上添加指向这些 IP 地址范围的路由。完成 IP 地址分配后，单击下一步。

在“管理多个远程访问服务器”中，如果用 RADIUS 进行份验证和授权，则单击是，否则单击下一步。由于我们需要基于轻量目录访问协议(LDAP)实现校园内的用户统一身份认证和授权，而 Windows 2000 VPN 服务器端本身无法直接支持 LDAP，因此这里我们设定需要使用 RADIUS 服务器，通过 RADIUS 服务器去访问 LDAP 上的用户数据。在 “RADIUS 服务器选择”中，指定主要、辅助 RADIUS 服务器的 IP 地址和共享密码，然后单击下一步。

然后单击完成。

按照以上步骤就启用了 Windows 2000 下的 VPN 服务。我们可以选择继续配置 PPTP 端口。PPTP 端口主要是用来调整同时访问 VPN 服务器的 VPN 客户数目。通过右键单击控制台目录树的“端口”，然后单击“属性”。在“端口属性”对话框中，单击“WAN 微型端口(PPTP)”，然后单击“配置”。在“最多端口数”中，键入端口数，然后单击“确定”。

值得注意的是在缺省情况下，VPN 客户端是无法连接到 VPN 服务器的，还需要修改缺省的远程访问策略。步骤如下：

单击控制台目录树的“远程访问策略”。

在窗口右边单击“缺省的远程访问策略”，选择属性。

采用缺省的条件和配置文件，设置如果用户符合上面的条件时“授予远程访问权限”。

4.2 客户端

客户端连接到 VPN 服务器分为两步。首先客户端要连接到 Internet，这一步和平时使用的各种连接到 Internet 的方法是一致的；其次是客户端要建立一个连接到 VPN 服务器，我们以 Windows 2000 Professional 为例说明，其他操作系统可参阅相关系统文档。步骤如下：

依次单击开始、设置、网络和拨号连接。

双击新建连接，然后单击下一步。

选择“通过 Internet 连接到专用网络”，单击下一步。

输入上一步启用 VPN 服务的 Windows 2000 主机外部网卡的 IP 地址，然后单击下一步。

选择是让所有用户都使用该连接还是只让自己使用，这里我们选择“所有用户使用此连接”，单击下一步。

输入为这个连接指定的名称，我们使用缺省名称“虚拟专用连接”，最后单击完成。

通过以上设置，我们完成了 Windows 2000 下的远程访问 VPN 服务端和客户端的配置。这样校外用户在访问校园内部网络资源时，不再需要象从前那样直接拨号到校内的电话，只需先连接到 Internet，然后通过 VPN 建立的虚拟专用连接就能直接访问校园内部网络资源。

参考文献

1 江魁等，深圳大学校园网 VLAN 解决方案[J]，小型微型计算机系统，2001，22：17－20。

2 Venkatesw aran R. Virtual Private Network[J]，IEEE Potentials，2001，20(1)。

3 戴有炜，Windows 2000 网络专业指南[M]，清华大学出版社，2000。