VPN 技术在校园网中应用的研究

张晓岗

(渭南师范学院计算机科学系03级3班)

摘 要：针对当前高校跨地域分布导致的校园网建设中所遇到的问题，文章结合VPN技术的特点，提出将VPN技术应用在高校网络的建设中，给出了一种基于VPN技术的高安全性网络解决方案，用于提供高效、安全、灵活和经济的网络数据传输，该技术的应用还可以提供可靠的校区互联、移动办公和校际交流三个方面的拓展功能。

关键词：校园网；VPN技术；虚拟专用网

1 引言

当今，随着互联网的迅速发展与普及，各高校也把校园网作为其基础的公共通信平台，校园网建设步伐不断加快。近几年来，由于高校合并、在异地设立分校等导致了校园呈现多校区化且跨地域分布，而且随着规模的扩大，出现了校区之间各种信息数据交流量庞大、利用网络的远程教育蓬勃发展、住在校外或出差的教师也有使用校园网的需求等问题，传统的单一校园网组网技术已不能满足要求。简单的处理方法是利用公共互联网互访，然而，这使校园网资源的安全性难以保障，如何高效、安全、低成本地交换数据，如何使地理及物理上分布分散的若干校区子网能从逻辑上有效集成，这些问题成为制约高校校园网建设和发展的一个瓶颈。

本文从这一问题出发，通过对VPN技术的具体分析和研究，提出了一种采用VPN技术解决高校校园网建设的方案。

2 VPN 简介

虚拟专用网VPN(Virtual Private Network) 是利用公众网资源为客户构成专用网的一种业务，这是相对于实际的专有网络而言的，它是基于 Internet/Intranet 等公用开放的传输媒体，通过加密和验证等安全机制建立虚拟的数据传输通道，以保障在公共网上传输私有数据信息不被窃取、篡改，从而向用户提供相当于专用网络的安全服务，是目前广泛应用于电子商务、电子政务、大型企业等应用安全保护的安全技术。 VPN 有两层含义：

1. Virtual ：它是虚拟的网，即没有固定的物理连接，网路只有用户需要时才建立；

2. Private ：它是利用公众网络设施构成的私有专用网。

虚拟专用网（ VPN ）代表了当今网络发展的最新趋势，它综合了传统数据网络的性能优点（安全和 QOS ）和共享数据网络结构的优点（简单和低成本），能够提供远程访问，外部网和内部网的连接，价格比专线或者帧中继网络要低得多。而且， VPN 在降低成本的同时满足了对网络带宽、接入和服务不断增加的需求，因此， VPN 的特性决定了它在教育行业的应用前景将非常广泛。

3 VPN 的技术原理

VPN 系统使分布在不同地方的专用网络在不可信任的公共网络上安全的通信。它采用复杂的算法来加密传输的信息，使得敏感的数据不会被窃听。其处理过程大体是这样：

1)要保护的主机发送明文信息到连接公共网络的 VPN 设备；

2)VPN 设备根据网管设置的规则，确定是否需要对数据进行加密或让数据直接通过；

3)对需要加密的数据，VPN 设备对整个数据包进行加密和附上数字签名；

4)VPN 设备加上新的数据报头，其中包括目的地 VPN 设备需要的安全信息和一些初始化参数；

5)VPN 设备对加密后的数据、鉴别包以及源 IP 地址、目标 VPN 设备 IP 地址进行重新封装，重新封装后的数据包通过虚拟通道在公网上传输；

6)当数据包到达目标 VPN 设备时，数据包被解封装，数字签名被核对无误后，数据包被解密。

4 VPN的主要技术

4.1 隧道技术

为了形成VPN链路，采用了“隧道”技术。网络隧道技术涉及3种网络协议，即网络隧道协议、隧道协议所承载的协议和隧道协议承载的被承载协议。使用隧道传递的数据（或负载）可以是遵守不同协议的数据帧或包。隧道协议将这些遵守其他协议的数据帧或包重新封装在新的包中发送，并对新的包提供了路由信息，从而使被封装的负载数据能够通过互联网络传递。被封装的数据包在隧道的两个端点之间通过公共互联网络传递，传递时所经过的逻辑路径称为隧道，到达网络终点时，数据包被解包并转发到最终目的地。

4.2 隧道协议

4.2.1 点对点隧道协议(PPTP)

PPTP 支持通过公共网络（如 Internet ）建立按需的、多协议的、虚拟专用网络。 PPTP 可以建立隧道或将 IP 、 IPX 或 NetBEUI 协议封装在 PPP 数据包内，因此允许用户远程运行依赖特定网络协议的应用程序。 PPTP 在基于 TCP/IP 协议的数据网络上创建 VPN 连接，实现从远程计算机到专用服务器的安全数据传输。 VPN 服务器执行所有的安全检查和验证，并启用数据加密，使得在不安全的网络上发送信息变得更加安全。通过启用 PPTP 的 VPN 传输数据就像在一个局域网内那样安全。另外还可以使用 PPTP 建立专用 LAN 到 LAN 的网络。 PPTP 协议捆绑在 Windows 系列操作系统中，在 VPN 中应用最广。

4.2.2 第2层隧道协议(L2TP)

L2TP 结合了 PPTP 和Cisco 公司 L2F 协议内容，支持封装的 PPP 帧在 IP, X.25, 帧中继或 ATM 等网络上传送。当用 IP作为 L2TP 的数据包传输协议时，可以使用 L2TP 作为 Internet 网络上的隧道协议。L2TP 还可以直接在 WAN 媒介上被使用而不需要传输层。

4.2.3 安全协议(IP Sec)

IP Sec 不是一个单独的协议，而是一组开放协议的总称，他对应于IP层的网络数据，提供一套安全的体系结构，包括网络安全协议 AH 和ESP、密钥交换协议 IKE 和用于网络验证及加密的算法等。IP Sec 规定了如何在对等层之间选择安全协议、确定安全算法和交换密钥，向上提供访问控制、数据源验证、数据加密等网络安全服务。

4.2.4 Internet密钥交换协议(IKE)

IKE 被用于两个通信实体的协商和安全相关的建立。安全相关表示两个或多个通信实体之间经过身份验证，均支持相同的加密算法，即可交换密钥，并利用 IP Sec 安全通信。IKE 定义了通信实体间身份认证、协商加密算法以及生成共享的会话密钥的方法。

4.3 加密和解密技术

VPN 技术的安全保障主要就是靠加密、解密技术来实现的，除了用隧道技术确保在两点或两端之间建立一条通信专用通道之外，两边的设备还必须增加建立于信任关系基础之上的加密、解密功能，虚拟专用网（ VPN ）使用的是标准

Internet 安全技术，进行数据加密、用户身份认证等工作。

在 VPN 中， IPsec 的安全性是最好的。在建立安全隧道和使用安全策略时，各个过程进行得更加严格。 IPsec 使用了 IPsec 隧道模式。在这种隧道模式中，用户的数据包加密后，封装进新的 IP 。这样在新的数据包中，分别以开通器和终端器的地址掩蔽用户和宿主服务器的地址。

4.4 密钥管理技术

密钥管理技术的主要任务是如何在公共数据网上安全地传递密钥而不被窃取。现行的密钥管理技术分为 SKIP 与 ISAKMP/OAKLEY 两种。

4.5 身份认证和安全策略

虚拟专用网（ VPN ）是一种通过 公众网资源为客户构成专用网的一种业务，如果安全技术不过关，势必给黑客造成可乘之机，将给使用它的用户带来不可估量的损失，所以说身份认证和安全策略是它的生命。在隧道建立过程中，采取一系列的步骤以保证数据在公共网络中传输的安全性。

(1) 用户认证：由于 VPN 跨越了无安全保障的公共网络平台，一些非授权的隧道建立请求和冒名连接的闯入不可避免。用户把姓名、口令通过增强用户握手认证协议（ CHAP — Challenge Handshake Authentication Protocol ），发送到 ISP 网络。 ISP 网络联系企业 RADIUS 服务器，进行用户确认，收到确认后， ISP 网络又以 CHAP 将应答传给用户。同时 ISP 收到企业服务器发回的用户 IP 及子网掩码分配，以及隧道终端器的 IP 地址分配。

(2) 进行设备确认：建立安全隧道。隧道开通器使用自己的私钥进行数字签名，并发送给隧道终端器，隧道终端器使用隧道开通器的公钥，对隧道开通器进行签名确认。反之，隧道开通器对终端器进行确认。然后双方协商对数据进行加密时使用的算法。

(3) 使用安全策略：下一步确认对本次传输的特定用户采取的安全策略。用户身份级别越高，消息认证等过程就越严格。

VPN 网络中通常还有一个或多个安全服务器。其中最重要的是远程拨入用户安全服务器（ RADIUS — Remote Authorization Dial-In User Service) 。 VPN 根据 RADIUS 服务器上的用户中心数据库对访问用户进行权限控制。 RADIUS 服务器确认用户是否有存取权限，如果该用户没有存取权限，隧道就此终止。同时 RADIUS 服务器向被访问的设备发送用户的 IP

地址分配、用户最长接入时间及该用户被允许使用的拨入电话号码等。VPN和访问服务器参照这些内容，对用户进行验证，如果情况完全相符，就允许建立隧道通信。

5 VPN的优点

5.1 成本低

VPN利用了现有的 Internet 组建虚拟专网，不需要使用专用的线路就能实现数据安全的传输，提供了比其它通信方式更低廉的成本。

5.2 易于扩展

在分部增多，内部网络结点越来越多时，专线连接网络结构趋于复杂，费用昂贵，而采用 VPN 只需在结点处架设 VPN 设备，就可利用 Internet 建立安全连接，如果有新的内部网络想加入安全连接，只需添加一台 VPN 设备，改变相关配置即可。

5.3 安全性强

安全是 VPN 技术的基础，为了保障信息的安全，VPN技术利用可靠的加密认证技术，在内部网络建立隧道，以防止信息被泄漏、篡改和复制。

6 VPN技术在高校校园网中的应用

当前，国内多数高校存在地理上跨地域分布，为了保证学校逻辑和管理上的统一性要求，导致了位于不同地域的校区间网络信息交换呈现出了信息交流量大、交换频率高和信息涉密程度大等特点，这就要求高校的校园网络体系必须满足分布性、高效性和安全性。网络既要保证高校运转，又要保证数据的绝对安全，此外，由于经费限制，还要保证建设和运行的低成本等，解决这些问题的关键在于如何实现不同校区间的子网互联。结合对于 VPN 主要技术及优点的分析，该技术恰好可以用来解决以上问题，应用于高校校园网络的构建，可以方便地提供校区互联、移动办公及校际交流等服务。

6.1 校区互联

在不同地域的分校区子网与主校区子网间或是分校区与分校区间，利用相应

的VPN设备，可以建立VPN

网络，一方面，使得各分校区与主校区间方便、安全地共享资源和进行数据交流，另一方面，VPN技术还提供了一种虚拟的专用网环境，使得原本在地域上相对分散校区的网络连成一体，在逻辑上保持了统一性；此外，还可以节省大量的建立专用网而必须支付的用于租用通信线路的费用。

6.2 移动办公

对于出差在外或是在家的学校工作人员，利用相应的VPN客户端软件，采用拨号方式或本地ISP，接入学校的VPN网络，可以实现传统物理专用网所不能实现的移动办公等功能，从而提高工作效率。

6.3 校际交流

在不同的多所高校间，往往存在着一些资源共享和信息交流的需求，在这样的高校间，基于一所高校，完全可以建立起该高校与多所高校间类似于企业扩展VPN的VPN网络，用于进行校际资源安全共享和信息的交流，而这一点，如果使用专用网络实现，其投入和成本都是不可接受的。

7 VPN技术应用于校园网方案

通过对网络的现状的分析可知，将VPN技术应用于校园网需要和校园网现有的两种网络结构相结合：远程访问网络(校园网用户在校外远程访问校园网)和学校内部的校园网，所以在现有校园网基础上建立 VPN 可以采用 Access VPN 和 Intranet VPN 两类，具体方案如图1所示。

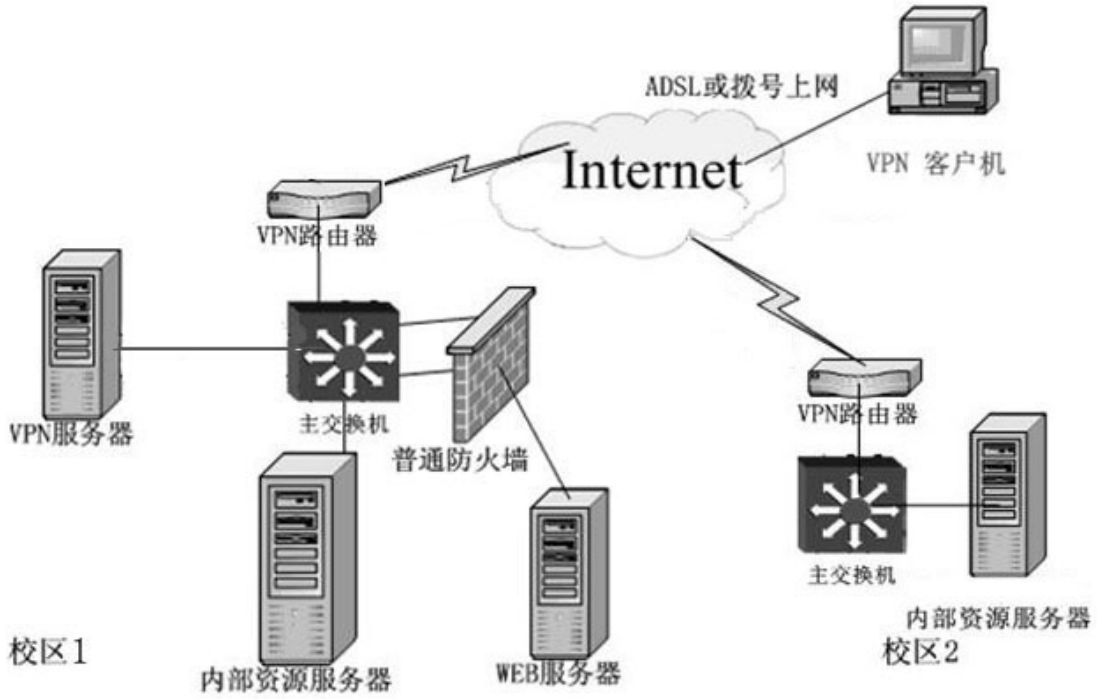

图1 校园网中的VPN应用方案

7.1 远程用户访问虚拟网(Access VPN)

从校园网的策略来讲，有些校园网资源是指允许校内用户访问的。在校外需要访问校园网内资源的远程用户的 IP 地址不是固定的，要使远程用户通过 VPN 接入校园网，一种方法是和 ISP 协商，由 ISP 提供隧道开通端的路由器，在校园网路由器上设置隧道终端，另一种方法是在用户端使用 VPN 功能的软件，配置为隧道开通器，通过 ISP 接入 Internet 并访问校园网内的 VPN 服务器。这里选择第二种方法，即在校园网内建立 VPN 服务器。

校园网络用户使用的操作系统平台多是 Windows 系列，而 Windows 2000 Server中的 RRAS (路由和远程访问服务)可以被用来建立使用 PPTP 或 L2TP 的 VPN 连接(包括路由器到路由器和用户远程访问服务器两种方式的VPN 连接)。因此选择在校园网内使用 Windows 2000 Server 建立 VPN 服务器，而终端用户只要在 Windows 系列的平台上配置 VPN 客户端，便可通过远程的 VPN 服务器访问校园专用网。在 Windows 中，VPN 连接都是作为使用 RAS(远程访问服务器)的拨号连接建立的。RAS 处理一个导入申请来建立一个 VPN 连接的方法很类似于处理一个与远程服务器的拨号连接。

因为建立一个远程访问的 VPN 服务器，