设计研究与应用

试论 VPN 技术在校园网络安全体系中的应用

王洪平
(南充职业技术学院电子信息工程系，四川南充 637131)

摘 要：现代化教育的发展与信息化密不可分，我国高校已经建设校园网，在校园内部开展基础性的管理工作。由于当前的公共网络环境有着明显的开放特征，因此校园网要想安全、稳定地运行，必须构建与之相关的安全体系。在建设校园网络相关安全体系的过程中，VPN 技术的应用十分关键。基于此，如何在校园网络体系之中合理应用 VPN 技术，需要我国高校进行深入研究。

关键词：VPN 技术；校园网络；网络安全体系；运用策略
中图分类号：TP309.5 **文献标识码：**A **DOI：**10.3969/j.issn.1003-6970.2022.05.041
本文著录格式：王洪平.试论VPN技术在校园网络安全体系中的应用[J].软件,2022,43(05):150-152

On the Application of VPN Technology in Campus Network Security System

WANG Hongping
(Department of Electronic Information Engineering, Nanchong Vocational and Technical College, Nanchong Sichuan 637131)

【Abstract】：The development of modern education is inseparable from informatization. Colleges and universities in my country have built a campus network to carry out basic management work within the campus. Since the current public network environment has obvious open features, the campus network must build a related security system in order to operate safely and stably. In the process of building a campus network-related security system, the application of VPN technology is very critical. Based on this, how to rationally apply VPN technology in the campus network system requires in-depth research in our country's colleges and universities.

【Key words】：VPN technology;campus network;network security system;application strategy

我国高校当前都已经建设自身的校园网络，以保证校园内部的所有信息以及资源都可以做到及时共享以及传送，进而打造出全新的信息化校园。伴随着我国高校在新时代办学规模的进一步扩大，分校区相继建立，而校园网内部的信息资源会受到保护，只有校园网的用户才能够访问。VPN 技术在得到应用之后，能够解决地域限制，保障校园网络的安全，同时使高校师生的需求得到满足。

1 VPN 内涵及其技术概括

1.1 VPN 相关内涵

VPN 是 Virtual Private Network 的缩写，翻译成中文为“虚拟专用网”。VPN 通过连接分布于不同区域的数个私有网络，进而形成逻辑层面的专用虚拟网络，组织网络外的探视和截听等活动，使传输的信息被加密，验证信息发送者的身份，避免身份被伪造，同时避免被传输的信息遭到篡改和泄露，使所有信息能够在网络内完整地传输。而且 VPN 技术最大的特点为远程访问，在构建专用网络的过程中，会利用现有的公共网络。例如，高校教职工可以通过远程访问功能，访问校园网的内网服务器并获取资源 [1]。

1.2 VPN 所运用的相关技术

（1）数据加密。在通常情况下，虚拟专用网络所运用的主要传输方法，就是对数据进行隐藏或者加密。如果数据在传输过程中，其所处的网络环境安全性较差，那么在数据进行传输的时候，即使用户的真实身份通过了验证，那么也难以保证 VPN 是否处于安全的环境中 [2]。因此，用户的真实身份在隧道端认证的同时得到加密，保证所有数据可以在加密之后传输；另一个端用于接受被传输的数据，用户在已经通过认证之后，对加密传输的数据信息进行解密，获得相对应的原始数据。上述技

作者简介：王洪平（1971—），男，四川嘉陵人，本科，副教授，研究方向：计算机网络、网络安全、计算机应用及算法。

术通常被分为两类，即对称加密以及非对称加密。

（2）访问控制。用户无论怎样访问系统，或者无论怎样使用系统所提供的资源，都会受到访问控制功能的管理。没有得到系统授权的用户会被系统“拒之门外”，无法进行访问。

（3）用户认证。虚拟隧道是数据得到传输的关键一环，在对用户身份加以仔细辨别及认证之后，就可以对用户访问系统资源的行为进行合理管控。要想对用户进行认证，应当利用哈希函数，变换数据提供的报文的长度，生成与报文内容和长度相同的摘要。然而，哈希函数是人们无法精确控制的，其特性会对报文造成一定干扰，如果人们想从海量数据报文之中，找到符合要求的报文摘要，必然会耗费大量时间以及精力，其工作难度较大 [3]。

（4）隧道传输。在 VPN 的传输之中，占据重要地位的技术就是隧道传输。隧道传输要想达成，必须将某个协议作为载体，使另外一类协议的数据传输得以实现，其应用本质主要为隧道协议，并大致分为传输、乘客、隧道三个方面的协议。在此之中，传输协议要想完成数据的传输任务，就必须与隧道的定义相结合；乘客协议会封装所有数据，无论是数据帧还是数据包，在协议之中都会存在一定差异，就必须封装数据帧以及数据包，然后才能够传输，所有数据在被封装之后到达目的地，中途不可以对数据进行解封，最终得到原始数据；隧道协议则主要为数据传输所需渠道的建设、保持以及拆除。

2 我国校园网络存在的重点安全问题

（1）来自网络外部或者内部的入侵攻击。校园网的开放性十分显著，会直接连接互联网，为高校师生的工作和学习提供便利，但是可能遭到攻击。由于校园网与企业网络不同，无法限制部分网页的浏览，以及对外部发起的连接请求加以拒绝，导致某些不法分子会对校园网发起攻击，并且入侵校园网，窃取校园网内部的资源和机密数据，或者破坏系统、篡改数据等 [4]。

（2）校园网系统自身存在一定漏洞，且可能遭受病毒入侵。连接校园网的计算机通常为 Windows 系统，该系统内部存在一定的安全隐患，例如服务器、操作系统、防火墙、TCP 或者 IP 协议等，如果上述漏洞没有被及时处理，计算机病毒就会乘虚而入。计算机病毒的主要特征为种类繁多、破坏性强、影响大、爆发时间不确定等，甚至导致重要文件丢失、整个系统崩溃等严重后果。不仅如此，高校师生在利用校园网下载软件、音视频等内容的时候，可能会将木马病毒带入校园网，导致校园网的安全性遭受威胁。

3 在校园网络安全体系应用 VPN 技术的策略

3.1 应用 VPN 技术的原则

要想在校园网络的安全体系之中应用 VPN 技术，就必须对校园网络的运用以及需求范围加以考虑，同时遵守 VPN 技术相关的应用原则。校园网络将 VPN 技术应用于安全体系的建设，通常分为以下四个模块：

（1）后台管理。在建设相应的后台之后，VPN 相关服务器之中的所有访问记录能够被收集，然后对记录加以整合，再传输至安全审计模块重新管理，通过后台功能对用户的操作行为以及详细情况进行总结 [5]。

（2）浏览控制。建设该模块的作用，就是与 VPN 技术的浏览控制方案相结合，保证技术系统自身具备有效设定，并针对客户需求精准送达相应的服务。

（3）身份验证。客户端内部的验证是十分必要的，而且服务和客户两个端口的认证方法并不相同，在内部网络之中加入数字认证技术，同时在外部网络的验证之中使用户及其密码得到结合。

（4）数据传输。其主要作用就是对所有传输的数据进行加密处理，这也是一种网络体系的核心，并且对数据进行转发。

当前，我国绝大多数高校会对应用 VPN 技术提出较高的要求，尤其是高校的财务部门以及后勤部门，所以，已经连接互联网的校园网，会将二层隔离作为主要工作方式，通过重心交换机传输所有数据，从而使各个分校区的任务得以顺利地传递。个别用户有着较低的安全级别，会使得安全级别层面的要求有所降低，VPN 技术相关的服务器性能也需要得到提升 [6]。

3.2 设计方案

3.2.1 主分校区构建校园内部虚拟专用网

对光纤线路进行运用，使高校地分校区与主校区相互连接，并且在分校区的校园网络内部设置相应的网络出口，如果想推行人事档案、学生考试成绩等相对应的应用系统，在正式投入运行的过程中，必然会利用光纤链路开展工作。上述链路之中传输的所有数据信息，可以通过 IPSec VPN 技术进行加密，从而使信息在网络之中能够安全地传递。普通的校园网用户在产生相应的访问请求之后，需要设置相对应的安全方式，从而使普通用户也能够访问校园网，无论是主校区还是分校区。如果设置了过高的安全等级，网络系统的资源会被大量浪费，还会影响用户的访问速度，导致整体访问速度被拖慢。

部分校园网的用户身处比较敏感的业务区块，例如

学生成绩的管理、财务管理、人事档案的管理等，就必须运用二层协议网络隔离这一形式，首先保证用户能够与校园网络相连接，然后将所有相关数据信息传递至校园网络内部的核心交换机中，从而使主校区以及分校区实现信息加密传输。不仅如此，主校区的校园网和分校区的校园网之间，必须配套相应的网络路由器，不同的校区在产生网络资源需求、相互传输数据的过程，会借助路由器完成。

3.2.2 VPN 服务器设置于校园网络内部

如果远程用户以及移动用户都在访问校园网，那么 VPN 所配套的软件系统就会发挥作用，封装并且加密数据。互联网服务由网络运营商提供，该服务的开放性极强，将其与校园网络的内网相连接，能够建设出专用的虚拟网络，也就是 Access VPN。无论是远程的还是移动的校园网用户，会发起连接请求，VPN 所配套的服务器对此进行连接。校园网络的使用系统选择 Linux，与 VPN 服务平台相配合，其原因是能够使操作系统具备更好的拓展性，且使用过程中有着更高的灵活度，操作也更加稳定。Linux 与 Windows 系统相比有着更强大的优势，在校园网络的内网之中增设 IBMX 366 服务器，Open VPN 软件均由 SSL 协议进行开发，因此在选择 VPN 服务器的过程中，应当选择优势更大的 Open VPN，从而创建出将 SSL 作为核心的 VPN 系统。

SSL 协议是构建 SSL VPN 的基准，可以帮助用户实现访问校园网的目标。在经过传输层之后，校园网络的地址会对设备进行转换，其中包括防护墙设备，从而使不同类型的用户都可以访问校园网。然而，无论是何种类型的用户，在发出访问请求之后，必须拥有校园网的 IP 地址才能访问。高校应当构建出一台 DHCP 服务器，并通过 DHCP 服务器，向所有用户提供可供其访问校园网络的 IP 地址。如果远程用户希望自身能够连接校园网络的服务器，就必须先获得其所配置的 VPN 服务器的域名 [7]。

我国高校可以通过增设域名的方式，增强服务器的效率，从而使用户能够准确地发出连接请求，并第一时间将其解析为 DNS 服务器的域名。远程用户在访问校园网的内部网络的时候，校园网会为用户提供一个专门的 URL 地址，用户发出网络连接请求，并且通过系统的身份验证，VPN 会根据该用户拥有的权限，进入指定的服务器内部。上述连接形式就是对专用的虚拟网络的远程访问，能够有效抵御来自外部网络的干扰，以及不法分子的恶意入侵。

4 结论

综上所述，校园网是高校建设信息化校园的关键部分，高校的不同校区要想做到无障碍相互连接，就需要科学应用先进的 VPN 技术，构建校园网络相关的安全体系。VPN 技术的应用可以妥善解决校园网络多个校区的接入问题，同时能够对校园网络内部的用户身份进行准确认证，加密传输所有数据信息。高校应当深入研究 VPN 技术，进而设计更适合自身发展的安全体系，使整个高校校园对于应用 VPN 技术的需求得到满足。

参考文献

[1] 邹力涵.高校网络中VPN技术的应用研究[J].科学技术创新,2018(23):60-61.

[2] 赵龙海.VPN技术在校园网络安全体系的应用研究[J].信息系统工程,2018(3):88+90.

[3] 刘璀,叶新恩,杨玲.基于SSL VPN技术的数字化校园统一认证平台研究[J].网络安全技术与应用,2018(12):91-92.

[4] 王岩红.基于VPN技术的校园网多场景安全保障策略研究[J].网络安全技术与应用,2021(10):97-98.

[5] 王真.VPN技术在校园网络安全体系的应用[J].网络安全技术与应用,2021(9):101-103.

[6] 刘淑影,曾涛,王静,等.校园网VPN系统的访问权限控制及其实现方法[J].重庆科技学院学报(自然科学版),2018,20(5):100-104.

[7] 张迎春.浅谈VPN技术在校园网中的应用[J].数码世界,2020(7):215.