文章编号：2096-1472(2020)-11-13-03
DOI:10.19644/j.cnki.issn2096-1472.2020.11.004

虚拟专用网技术在校园网应用中的研究与实现

刘邦桂

(广东开放大学人工智能学院，广东 广州 510091)
✉liubanggui@qq.com

摘 要：随着网络新技术的发展，在各高校全面打造数字校园过程中，基于网络的业务种类和形式不断增加，以传统网络技术为主要通信手段的校园网发展遇到了各种瓶颈，加上校区分散、管理相对独立等环境，基于SSL(安全套接字)协议的VPN(虚拟专用网络)技术在校园网的应用变得越来越重要，本文从VPN技术分类开始，详细分析了SSL VPN的实现原理，利用UTM设备实现了SSL VPN在我校的全面应用，对于提升企事业单位信息化办公效率，具有积极示范意义。

关键词：SSL协议；VPN技术；数字校园；UTM
中图分类号：TP393.2 **文献标识码**：A

Research and Implementation of Virtual Private Networks Technology in Campus Network Application

LIU Banggui

(*School of Artificial Intelligence, the Open University of Guangdong*, *Guangzhou* 510091, *China*)
✉liubanggui@qq.com

Abstract: With the development of network technology, network-based activities keep increasing in the building of digital campus throughout colleges and universities. The development of campus network with traditional network technology as the main communication means has encountered various bottlenecks. To make matters worse, college campuses are scattered and their management is relatively independent. Therefore, application of VPN (Virtual Private Network) technology based on SSL (Secure Socket Layer) protocol in campus network is becoming increasingly important. Starting from categorization of VPN technology, this paper analyzes the implementation principles of SSL VPN in detail. Equipment of UTM (Unified Threat Management) is also used to realize full application of SSL VPN in universities, which significantly improves the effectiveness of information-based office work in enterprises and institutions.

Keywords: SSL protocol; VPN technology; digital campus; UTM

1 引言(Introduction)

通信技术和计算机网络技术的不断发展，特别是5G技术、大数据等新技术的出现，如何在高速通信链路上安全地传输大量私密数据变得越来越重要，网络安全的重要性慢慢在大家日常学习、生活、工作中体现出来。目前各种企事业单位有总部、分部、外出办事、合作机构等各种形式组成，在日益流行的无纸化办公模式，结合不断增多的日常内部办公文件的大环境下，大部分企业通过专网、发布在公网各类服务器、网络存储等形式来实现。然而，在实际使用过程中，如何在数据安全性、员工工作效率、网络技术管理成本等方面，寻找一个平衡点，是大部分企事业单位面临的重点和难点。

虚拟专用网是解决通信安全问题的有效方式，是目前信息安全领域重要研究领域之一[1]。虚拟专用网技术以共享公共网络为基础，以虚拟而非物理连接来构建私有的专用网络，而且处于私有的管理策略之下，具有独立的地址和路由规划，整体来看相当于穿过一个混乱的公共网络，形成一个安全而又可靠的隧道，实现各个网络的统一。目前，对于高校来说，多校区、多业务协同、分布式工作的业务很多，教务、图书资源、财务、人事、校园一卡通、学生等系统被广

泛应用，合理利用VPN技术来搭建以上服务，为全校师生提供工作和学习的便利，是目前高校校园数字化、信息化建设过程中的一种必然趋势。其中SSL VPN(基于安全套接层的虚拟专用网)也因其安全性和易用性在安全传输中得到广泛使用[2]，本文就基于SSL协议的VPN技术在我校的应用进行研究。

2 VPN 技术(VPN technology)

2.1 VPN技术分类

VPN技术有以下几种分类：(1)按业务用途分为：Access VPN、Intranet VPN、Extranet VPN；(2)按照运营的模式分为：CPE-Base VPN、Network-Based VPN；(3)按照组网模型分为：VPDN、VPRN、VLL、VPLS；(4)按照网络层次来分：Layer 1 VPN、Layer 2 VPN、Layer 3 VPN、传输层 VPN、应用层VPN。其中主要的二层VPN技术有：L2TP(Layer 2 Tunneling Protocol)VPN、PPTP(Point to Point Tunneling Protocol)VPN、MPLS(Multiprotocol Label Switching)L2 VPN；三层VPN技术有：GRE (Generic Routing Encapsulation)VPN、IPsec(Internet Protocol Security)VPN、BGP(Border Gateway Protocol)VPN。

2.2 SSL VPN技术

SSL是在因特网基础上提供的一种基于WEB应用的保证私密性的安全协议[3]。它能提供数据加密功能，用数字签名技术对通信双方身份验证，抗中间人攻击，防御密码回滚攻击等[4]。

Netscape公司为了保证浏览器与Web服务器之间数据传输的私密性，开发了具有数据加密功能的通信协议SSL 1.0，在1996年推出了功能和安全性都比较完善的SSL 3.0。SSL协议是一种TCP服务，监听443端口，对上层提供端到端、有链接的加密传输服务，同时使用了C/S架构通信模式。SSL协议包含两层：(1)SSL记录协议。主要作用为向高层协议提供服务、对数据进行打包、加密和压缩等，这些作用为整个网络系统中的基本功能。(2)SSL握手协议。该协议的位置在记录协议之上，在正式的数据传输过程开始前，需要对该协议进行合理应用，在正式的数据传输工作开始前，该协议会开展身份认证、密钥交换和加密算法协商工作[5]。SSL协议有三种握手过程：(1)无客户端认证的全握手过程，在该过程中服务器端不验证客户端身份。(2)有客户端身份认证的全握手过程，可以通过此过程利用数字签名来验证用户身份[6]。(3)会话恢复过程，握手过程涉及较多复杂算法，SSL协议提供了会话恢复机制，使得后面建立的连接可以利用当前会话参数，避免重新协商的过程，提高建立连接的效率。

2.3 SSL VPN 产生背景

VPN技术分类中最早出现加密功能的是IPsec VPN，虽然其简单高效，但是在接入过程中网络互联性不好，在客户端用户使用和维护要有一定的技术，带来了管理方面的不便，访问权限管理方面也比较粗糙。对于以上IPsec VPN的弱点，SSL VPN有良好的表现：(1)SSL工作在TCP层，不受NAT技术和防火墙的限制[7]。(2)借助浏览器来实现客户端的自动安装和配置，减少了客户端的维护。(3)解析应用层协议，进行高粒度的访问控制。其他详细比较，见表1。

表1 IPsec VPN与SSL VPN的比较

Tab.1 Comparison between IPSec VPN and SSL VPN

远程访问的安全需求		IPsec VPN	SSL VPN
安全性	传输加密	各种常见算法	各种常见算法
	身份认证	种类少，强度不高	种类多，强度高
	权限	粒度粗	粒度细
	防病毒	难以实施	可以实施
易于接入	访问地点	网络互联性不好	网络互联性好
	设备需求	客户端兼容性不好	客户端兼容性好
易于使用	免安装	需要预先安装	免安装或自动安装
	免维护	手工配置	自动配置
易于集成	认证集成	支持的种类少，与原有认证系统较难集成	支持的种类多，与原有认证系统易于集成
	应用集成	支持各种IP应用	支持各种IP应用

能够简单安全高效地使用网络服务才是客户在选择VPN技术的重点。客户一般知识不够，对通信设备掌握也不多，为了实现远程办公，要简化网络的接入过程，降低操作难度，又经济安全实惠，并且能够提高用户的可操作性与企业整体的办公效率，SSL VPN就成为各单位的首选。

3 SSL VPN的实现原理(The implementation principle of SSL VPN)

SSL VPN的首要功能就是为远程用户提供访问网络内部资源的手段。目前支持三种接入方式。

3.1 Web接入

用户只通过浏览器就能访问到内部网络资源的远程接入方式，如图1所示。SSL VPN网关公网地址是IP0，可以被远程主机访问到。内部的资源服务器Server A使用的地址是IP1，IP1是私网地址，远程主机无法直接访问到。远程用户通过Web浏览器与SSL VPN网关(IP0)之间建立SSL连接，通过SSL连接发送http请求，请求的地址是“https://IP0/ServerA”，这个URL并不是一个真实的路径，而是VPN网关给内网服务器ServerA建立的虚拟路径。VPN网关解析http请求，将报文中的请求路径“IP0/ServerA/dir1/page1”修改成为“IP1/dir1/page1”，将修改后的请求报文通过TCP连接转发给ServerA(IP1)进行处理。ServerA处理完远程主机发来的http请求后，返回应答报文。该报文一般情况下是一个web页面。Web页面文件中的连接<A>…</A>指向的是一个个内网服务器上的地址，如“http://IP1/dir2/page2”，这个URL是指向ServerA上的路径“/dir2/page2”的。这个地址对远程主机来说是不可访问的。VPN网关解析ServerA返回的Web页面，对页面中的链接逐一修改，使之映射成为外网可见的URL地址。如图1所示，将“http://IP1/dir2/page2”改写成为“https://IP0/ServerA/dir2/page2”。这样被改写过的页面传回给远程主机后，远程用户就可以访问页面中的链接了。

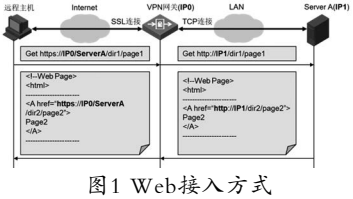

图1 Web接入方式

Fig.1 Web access mode

使用这种接入方式的最大好处就是“免客户端”，但这种方式主要适用于访问Web站点，对使用其他协议的网络应用则不支持。

3.2 TCP接入

用户可以使用原来的TCP应用客户端，透明地通过SSL VPN网络，访问内网TCP服务的远程接入方式，如图2所示。VPN客户端在远程主机上安装和运行起来后，会在Windows的hosts文件中设置一些静态的主机名解析表项，将内网主机名指向环回地址，如127.0.0.3 ServerA。这样远程主机上的应用程序在访问主机名为ServerA的设备时，将向127.0.0.3这个地址发出请求。而这个地址是一个本地地址，VPN客户端就监听在这个地址上，以接收应用程序发出的请求。应用客户端向ServerA发出建立TCP连接的报文。经远程主机对主机名ServerA的解析，确定发送的报文应当发送给127.0.0.3这个地址。VPN客户端正监听在127.0.0.3相应的端口上，收到应用客户端建立TCP连接的请求后，VPN客户端以代理的方式返回TCP连接建立的应答，在应用程序与VPN之间就建立起了一条TCP连接。VPN客户端与VPN网关之间建立起一条新的SSL连接。VPN网关与服务器ServerA之间建立起新的TCP连接。这样从远程主机上的应用程序客户端到内网的服务器ServerA之间就建立起了一条通道，该通道由三端连接首尾相接而成。通过这条通道，应用程序的客户端就可以同服务器之间像使用一条TCP连接那样进行数据的传输了。

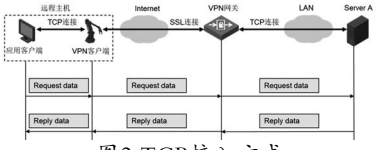

图2 TCP接入方式

Fig.2 TCP access mode

这种接入方式比较适合访问固定IP和固定端口的TCP服务，对动态协商通讯端口的网络应用，此种接入方式支持起来比较困难。

3.3 IP接入

一种实现远程主机与内部网络之间进行IP层互联的远程接入方式，如图3所示。首先需要在SSL VPN网关上配置一个为IP接入所使用的IP地址池。如1.1.1.1—1.1.1.255，建立一个虚接口sve1/0，配置IP地址1.1.1.1。在用户采用IP接入时，SSL VPN会通过Web页面在远程主机上下载并安装一个IP接入客户端和一个虚拟网卡。在虚拟网卡上，配置一个由SSL VPN网关分配的内网IP地址，图3中所示的1.1.1.100。在远程主机上，VPN客户端设置若干条路由，这些路由设置了允许该用户访问的IP网段。而路由的下一条都指向SSL VPN网关上的虚接口地址。192.168.1.0/24 1.1.1.1VPN客户端与SSL VPN网关之间建立起一条SSL连接。在Server A上配置默认网关指向VPN网关。通讯过程为：应用客户端要访问内网服务器Server A，已知Server A的IP地址是192.168.1.100，于是向该地址发送一个IP报文，该IP报文的目的地址是192.168.1.100，源地址是1.1.1.100；在转发该IP报文时，远程主机查询本地路由表，得知应该IP报文应该发送给默认网关1.1.1.1。而去往1.1.1.0网段的报文应该交给虚拟网卡处理；虚网卡接收到IP报文后，交给VPN客户端转发给SSL VPN网关；在SSL VPN网关上，IP报文被送到虚接口sve1/0。从此处再按照目的地址192.168.1.100进行路由转发，IP报文被送到了Server A。Server A的回应报文源地址是192.168.1.100，目的地址是1.1.1.100。该报文通过查找本地的路由，将报文发送给VPN网关；在VPN网关上，查找本地路由，得知IP报文应该发送给远程主机上的虚网卡，通过相应的SSL连接将报文发送给了VPN客户端程序；VPN客户端将IP报文发送给虚拟网卡，IP报文经由虚拟网卡上送到远程主机的TCP/IP协议栈，最后送达应用客户端程序。

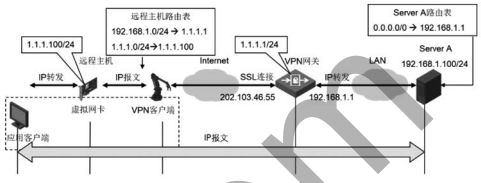

图3 IP接入方式

Fig.3 IP access mode

使用这种接入方式可以支持任何基于IP协议的网络应用，但这种方式需要安装比较复杂的客户端软件，在跨平台性和可维护性方面较弱。

4 SSL VPN的权限管理(Privilege management of SSL VPN)

SSL VPN权限管理可分为两大部分：静态授权和动态授权，如图4所示。

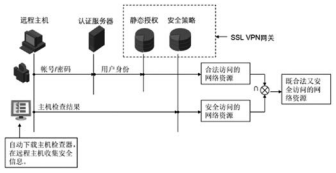

图4 权限管理

Fig.4 Authority management

4.1 静态授权

根据用户的身份授予用户相应的访问权限，主要解决访问权限的合法性问题。这种授权方式只与用户的身份有关，无论用户何时何地登录都拥有相同的访问权限。静态授权涉及主要技术有身份认证和静态权限管理。

为了便于同已有的认证系统集成，SSL VPN产品一般支持多种认证方式。其中包含本地认证和外部认证。本地认证是用户的账号和密码保存在网关本地数据库中，由网关独立地对用户身份进行认证。外部认证是用户的账号和密码保存在外部服务器上。在接收到用户提交的账号和密码后，网关将其交给外部服务器进行验证。网关根据服务器返回的验证结果决定是否允许用户登录SSL VPN。SSL VPN还支持证书认证、动态令牌认证、短信认证等目前流行的高级认证手段。

静态权限管理是把用户和用户组与资源和资源组进行关联，实现不同用户对应不同的资源组，达到权限管理的目的，一般是以用户组和资源组为单位进行设置。

4.2 动态授权

不仅要根据用户的身份，还要根据远程主机的安全状态确定用户可以安全地访问哪些网络资源。这样即使是同一用户，由于所使用远程主机的安全状态不同，被授予的访问权限也有可能不同。动态授权涉及的主要技术安全策略和主机

检查。安全策略是指如何定义安全状态，如何授予相应的管理权限，在SSL VPN系统中，安全策略用于定义远程主机所处的安全状态，以及在相应的安全状态下，远程主机可以安全访问的网络资源。主机检查远程主机的安全状态。通过下载一个客户端程序对远程主机的安全状态进行检查，并将相关信息反馈给SSL VPN网关，网关可以对远程主机的安全状态进行评估，确定它的安全级别。

5 SSL VPN的实现(Implementation of SSL VPN)

广东开放大学是全国六所开放大学之一。目前有19所市级开放大学、69所县级开放大学、20余所行业学院(分校)、自身有3个校区。各市县开放大学、自身各部门都需要在各校区共同访问网络应用系统，包括教务管理、财务管理、一卡通管理、图书馆管理等系统，以光纤链路在主校区与分校区之间建立虚拟专用网，并用IPSec VPN技术加密校区之间传输的数据，可以实现三个校区、市县分校之间进行数据加密互访，理论上能够满足网络业务需要，但是维护成本较高，特别是对市县电大客户端网络管理员技术要求比较高，为此采用了SSL VPN来部署各应用系统。

在广州校本部部署一台新华三技术有限公司的H3C SecPath U200-M作为SSL VPN服务器，三个校区、各市县开放大学、出差员工以公网的形式与SSL VPN网关建立VPN隧道，实现数据的加密传输。如图5所示。

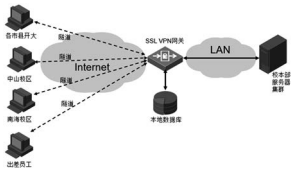

图5 网络拓扑图

Fig.5 The network topology diagram

在服务部署的过程中，有三类资源，教务管理、财务管理、校巴订票等WEB应用系统采用了WEB连接；公共文件共享比如FTP、远程桌面，采用TCP连接；办公室打印等采用IP连接。同时也设置了病毒防护、URL过滤、漏洞攻击防护、垃圾邮件防护、P2P/IM应用层流量控制和用户行为审计等安全功能[8]。

6 结论(Conclusion)

目前技术革新速度之快，对我校对信息化提出了新的要求。随着学校招生人数和教学规模不断扩大，多校区、多教学点管理模式的大环境下，通过VPN技术解决了校园网多校区的接入问题，使分校区和校外用户可以随时随地通过VPN通道访问校园网各种资源，确保了各校区之间的用户身份认证和数据加密传输。VPN技术在校园网的应用促进了我校智慧校园的发展，在校内部管理和教学活动管理的过程中，具有积极有益的意义。

参考文献(References)

[1] 唐鹏毅,李国春,余刚,等.基于QS-KMS的VPN增强电网通信安全方案[J].计算机工程,2018,44(12):13-17.

[2] 王琳,封化民,刘飚,等.基于混合方法的SSL VPN加密流量识别研究[J].计算机应用与软件,2019,36(2):315-322.

[3] 杜理明.基于SSL VPN技术的无线校园网的设计研究[J].集宁师范学院学报,2017(3):30-33.

[4] 何宛玲.基于SSL协议的VPN技术与应用[J].信息与电脑,2020(3):146-148.

[5] 汪志勇.对SSL VPN安全关键技术的运用[J].无线互连技术,2019(9):21-22.

[6] 陈海倩,张丽娟,赖宇阳,等.基于SSL VPN技术的电力安全网关设计与实现[J].电子设计工程,2020,28(13):97-100.

[7] Muc A, Muchowski T, Murawski L, et al. Providing the Ability of Working Remotely on Local Company Server via VPN[J]. Multidiplinary Aspects of Production Engineering, 2020,3(1):195-205.

[8] 张涛,芦斌,李玎,等.一种基于软件定义网络的主机指纹抗探测模型[J].信息网络安全,2020,20(7):42-52.

作者简介：

刘邦桂(1983-)，男，硕士，讲师.研究领域：服务器技术，网络安全技术.

(上接第33页)

学助手应用软件平台的开发，为学生提供了寓教于乐的移动学习平台，很好地践行了快乐学习与随时随地学习的理念，作为传统教学模式强有力的补充，满足了不同层次的学生的学习需求，通过教师科学的引导有助于学生更好的自我规划，使其在走上工作岗位之后仍能保持学习意愿，普及终身学习的理念。

参考文献(References)

[1] 程瑶.初探Android移动学习系统的开发[J].农家参谋,2019(17):208;212.

[2] 徐杰.“乐学堂”移动游戏化学习社区的构建与应用研究[D].云南师范大学,2019,5.

[3] 施冬梅,孙翠改,赵炜霞.基于泛在技术+Android Studio课程移动学习平台开发研究[J].镇江高专学报,2019,32(01):97-99.

[4] 王欣蕾.高职英语移动学习平台构建研究[J].科教文汇(下旬刊),2019(07):179-180.

[5] 刘锦.基于Android的移动学习APP的设计与实现[J].信息与电脑(理论版),2019,31(18):87-88;91.

[6] 翰建林.基于Android的移动学习平台的研究与设计[J].电子技术与软件工程,2018(4):47-48.

[7] 张济先.基于Android移动学习平台的设计与实现[J].现代工业经济和信息化,2019,9(3):38-39.

[8] Florian Malard, Philippe Grison, Louis Duchemin, et al. GOTIT: A laboratory application software for optimizing multi-criteria species-based research, 2020,11(1):159-167.

作者简介：

施冬梅(1976-)，女，硕士，副教授.研究领域：移动应用开发，PHP开发.

孙翠改(1982-)，女，硕士，讲师.研究领域：移动应用开发，人工智能.

盛雪丰(1981-)，男，硕士，副教授.研究领域：移动应用开发，人工智能.