VPN 技术在双校区校园网建设中的应用研究

Research on the Application of VPN Technology in the Construction of Dual Campus Campus Network

李军旺 LI Jun-wang
（岳阳职业技术学院，岳阳 414000）
(Yueyang Vocational Technical College, Yueyang 414000, China)

摘要： 根据双校区校园网建设的需求，本文提出了一种 IPSec+MPLS+SSL 相融合的方案，该方案综合了 IPSec、MPLS、SSL 技术的优点，经测试，该方案在保证安全的基础上，用户接入方便、灵活，有一定的扩展性，较好地满足了校园网设计需求。

Abstract: According to the requirements of the construction of campus network of the dual campus , this article proposes a solution which integrates IPSec+MPLS+SSL. After testing, this solution can make user access convenient and flexible while ensuring security. It not only has certain scalability, but also meets the design requirements of the campus network in a better way.

关键词： VPN 技术 双校区 数字校园

Key words: VPN technology ; dual campus ; digital campus

中图分类号：TP393.1　　**文献标识码：**A　　**文章编号：**1006-4311 (2023) 29-112-03　　doi:10.3969/j.issn.1006-4311.2023.29.036

1 VPN 技术

VPN 是虚拟专用网的简称，是一种利用共享的公共网络搭建虚拟的专用网络的技术。因传输数据的通道是运用“隧道”技术虚拟出来的，所以称为虚拟网。VPN 网络仅供合法的 VPN 用户专门使用，因此称为专用网。与其他专用网络相比，运用 VPN 技术实现远程访问，安全性、可靠性有保障且成本低、组网灵活、易于扩张、维护方便，因此得到了广泛的应用[1]。

2 VPN 的关键技术

一条 VPN 连接一般包括客户机、隧道和服务器三个部分。其工作过程一般是客户机将明文信息发送到与之相联的 VPN 设备，VPN 设备根据预先设定的规则，判断是否对其进行加密处理，对需要处理的数据，VPN 设备根据规则进行加密、认证并封装成一个新的数据包，新的数据包通过公网传输到达目标 VPN 设备时，数据包被解封、认证、解密，还原成原始明文信息发送给服务器。VPN 工作过程如图 1 所示。

图 1 VPN 工作过程

工作过程涉及的主要技术有隧道技术、认证技术、数据加密技术以及访问控制技术[2]。

2.1 隧道技术

所谓隧道是指通过封装、解封装技术在收、发双方之间建立的一条虚拟的数据传送通道。隧道技术是一种数据包封装技术，包括数据封装、传输和解封装的全过程。它是将用户数据包以数据净荷的形式封装成另一个数据包，然后通过隧道发送。中间的路由过程由新的数据包的包头决定，到达目的地后再通过解封恢复原始数据包。

隧道是由隧道协议形成的，为了建立隧道，通信双方采用的隧道协议必须相同。一个隧道协议包括乘客协议、封装协议、承载协议三种协议。乘客协议是被封装进数据包中的协议。封装协议的功能就是建立、保持以及拆除隧道等。承载协议是承载经过封装后数据包的协议等。

2.2 认证技术

包括身份认证与数据认证。在隧道启动前，要对用户的身份进行认证，确保只有合法的用户才可访问系统，不同权限的用户访问不同的资源。常用的认证方式有用户名+密码、USB KEY 等。数据认证技术主要采用摘要技术，利用 Hash 算法理论结果的唯一性和不可逆性，判定数据在传输过程中是否被篡改。

2.3 数据加密技术

数据被封装入隧道时进行加密，到达目的地后解密。加密是利用数学方法将明文转换为密文的过程。加密技术确保数据在隧道中传输过程中不被非法窃取，或者即使被窃取不明白信息的含义。加密或解密时用到的参数称为密钥。加密、解密采用同一密钥，称为对称加密。加密与解密采用不同的密钥称为非对称加密。

2.4 访问控制技术

通过访问控制技术确保只有授权的用户才能访问系统资源，不同权限的用户访问不同的资源，未授权用户不能访问资源。

3 常用 VPN 技术研究

3.1 IPSec VPN

IPSec 不是某一种具体的协议，而是 IETF 为保证 IP 层的安全通信（端到端 IP 报文交互的真实性、完整性、机密性、抗重放性）而制定的协议簇。

3.1.1 IPSec VPN 体系结构

IPSec 协议基于安全策略对不同的数据包采取不同的保护措施。IPSec VPN 体系结构主要涉及 AH（报文头验证协议）、ESP（封装安全载荷协议）和 IKE（因特网密钥交换）三个协议。AH 的主要功能是数据完整性校验、数据源验证、防报文重放。ESP 除提供数据完整性校验、数据源验

作者简介：李军旺（1975-），男，湖南岳阳人，硕士，讲师，研究方向为计算机网络技术。

证、防报文重放功能外，还提供加密功能[3]。IKE 是 IPSEC 的信令协议，主要功能是自动协商密钥、更新密钥、安全参数如何协商等。IPSec VPN 体系结构如图 2 所示。

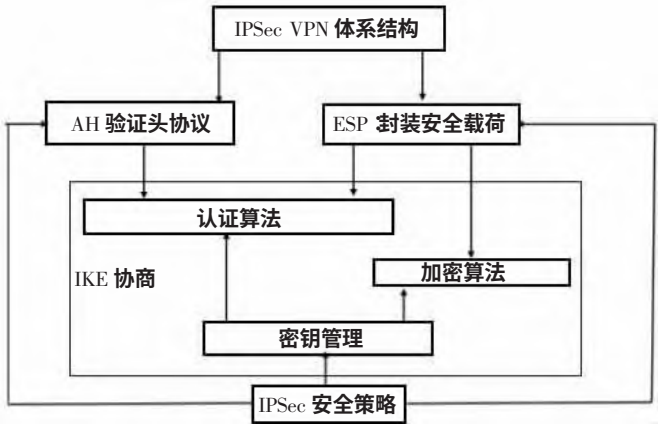

图 2 IPSec VPN 体系结构

3.1.2 工作模式

对 IP 数据包，IPSec 可以加密，也可以进行认证，还可以同时进行认证和加密。其工作模式有两种，传输模式和隧道模式。在传输模式时，IPSec 报头插入 IP 头部与 TCP 头部之间，同时 IP 报文中的协议字段数值改为 50 或者 51（50、51 是 IPSec 的协议号）。

传输模式下的报文格式如图 3 所示。

在隧道模式时，IPSec 报头插入在原 IP 头部的前面，IPSec 报头与原 IP 分组一起被当作有效载荷的一部分封装在新的 IP 报文中，这样原 IP 头信息被隐藏起来，安全性更好。但因要插入一个额外的新 IP 头部，故需要占用更多的带宽[4]。隧道模式下报文格式如图 4 所示。

3.2 SSL VPN

SSL（安全套接层）是一种基于 WEB 应用的安全协议。SSL 提供的服务一是对数据进行加密。二是确保收到的是没有更改的数据。三是对用户和服务器的身份进行验证，以确保收到数据是正确的客户端和服务器。认证采用数字证书，包括单向认证和双向认证两种。单向认证只需在服务器端安装 SSL 证书，任何用户都可以去访问。通常，基于 Web 的应用程序使用 SSL 单向身份验证。SSL 双向认证要求服务端和客户端都具备 CA 证书，在协议认证过程中，客户端和服务端会彼此校验对方的证书是否有效。使用双向认证可以加密被传输的信息，防止信息泄露，还可以在一定程度上增加服务端的信任度。

3.3 MPLS VPN

MPLS 是多协议标记交换的简称，采用标记（Label）交换且支持多种链路层与网络层协议。MPLS VPN 是 MPLS 技术应用的一个分支，通过 IP 骨干网络构建公司或企事业单位 IP 专用网络，以实现跨区域、高效、可靠、安全的多业务通信。MPLS VPN 网络通过在报文中插入 Label 来区分数据流，一个 Label 与一个用户数据流相对应，很容易实现隔离。各数据包根据 Label 进行转发，当到达 VPN 的边缘时，再由三层设备完成路由。MPLS VPN 主要包括运营商网络与用户网络二个部分，如图 5 所示。

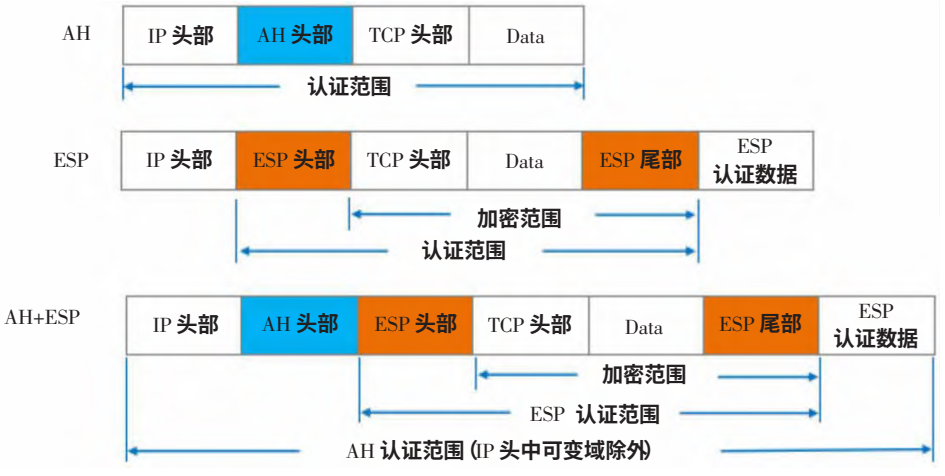

图 3 传输模式下报文格式

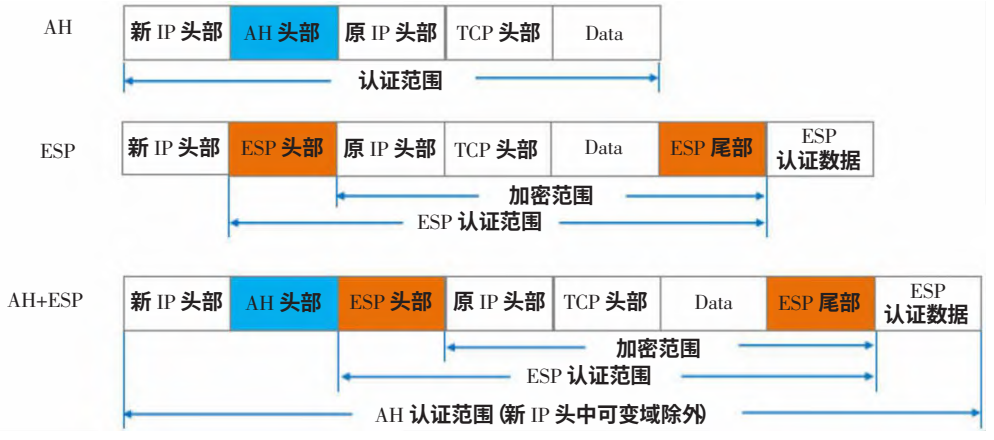

图 4 隧道模式下报文格式

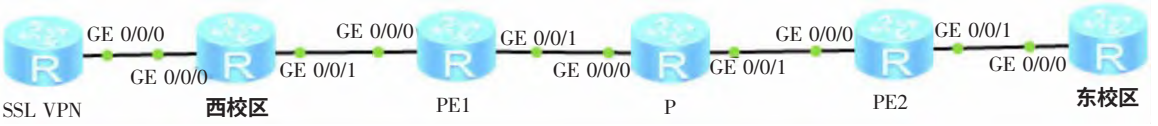

图 6　双校区数字校园拓扑图

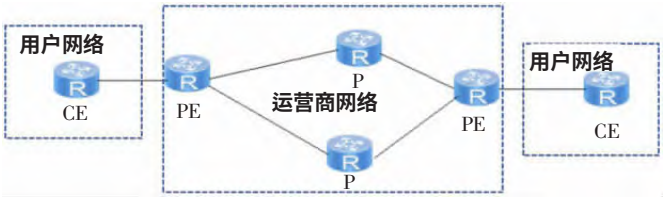

图 5　MPLS VPN 组成

其中运营商网络是 MPLS 的骨干网，由运营商管理并提供服务，P (Provider) 路由器根据标签 (Label) 进行分组的交换或转发，无需维护 VPN 信息，仅需具备基本 MPLS 转发能力即可。CE (Custom Edge) 是用户网络的边缘路由器，由用户配置，可以不支持 MPLS。PE 路由器是运营商网络与用户网络通信的桥梁，PE 路由器中不仅包括骨干网络的路由信息，也包括每一个 VPN 的路由信息，必须支持 MPLS 且要开启 MPLS 功能，VPN 配置与处理主要在 PE 路由器中完成。

3.4 各种 VPN 技术比较

①IPSec VPN 优点是只需在客户端的网关上进行部署，因此可以快速部署并投入使用；支持预共享秘钥验证或证书认证，因此安全性高。缺点是仅支持 IP 封装，不支持其他协议；需要特定的客户端支持不太适合移动用户；配置复杂，因此对管理人员的技术要求比较高；工作在第三层，很难穿越 NAT 和防火墙，访问一些安全措施较严密的系统时，容易出现访问受阻的情况[5]。

②SSL VPN 优点是只要有支持 SSL 的浏览器，无需安装、配置客户端就可以使用 VPN；封装的是应用层数据，因此能绕过防火墙和代理服务器访问内网资源；支持用户名/密码或证书认证，能够实现端到端的安全；可以对远程接入用户进行较精细的资源访问控制。SSL VPN 的缺点是不能对通信双方的主机间通信进行加密，只能对某个应用通道进行加密，故对资源提供的安全保障有限。

③MPLS 是天然的隧道，丢包率、时延有保障，无需配备专用的 VPN 设备，只使用一般的路由器就可以构建 VPN。但 MPLS VPN 一般由一家运营商提供的，跨运营商互联互通不理想，不支持用户认证和数据加密。

4　VPN 技术在双校区校园网建设中的应用

4.1 双校区校园网建设需求

某高校有东西两个校区，近年来，随着教育信息化的发展，数字校园上部署了与教学、学籍、办公、财务、人事、科研以及管理有关的多种应用系统，由于前期规划的问题，各种流量均通过专线传输，核心设备压力大。整个校园网可扩展性不强，每增加一项新业务，IP 地址的重新规划、网络设备的配置都比较麻烦，运维难度大、安全隐患多。网络改造后，一是要求用户接入方便、灵活，通过认证的师生能在校园内、外随时随地接入内部网络，进行成绩查询、图书馆资源访问；二是校园网的基础架构要有一定承载性，满足一定的在线教学、视频会议的需求，要求具备高带宽、高稳定性；三是要采用统一的安全策略，确保内网安全以及 Internet 访问安全[6]。

4.2 双校区校园建设方案

根据建设需求，结合前文 VPN 技术的研究与分析，提出了一种 IPSec+MPLS+SSL 的方案，东西两校区之间的互联通过 MPLS+IPSec 两种 VPN 技术相结合的方式。SSL VPN 服务器部署在西校区，以满足教职工、学生的校外访问与移动终端访问。用 eNSP 进行模拟测试，拓扑结构如图 6 所示。

IP 规划如下：校园网各业务、SSL VPN 服务器全部部署在西校区，IP 地址为：192.168.137.0/24；出口路由器 IP 为 172.18.1.1/24、SSL VPN 的 IP 为 192.168.1.2/24。东校区 IP 为：198.168.1.0/24，出口路由器 IP 为：172.18.2.1/24。

4.3 VPN 配置关建代码

IIS VPN 采用图形界面进行配置。MPLS VPN 配置时，PE 及 PE 两边接口都启用 MPLS、创建 MPLS LDP，具体配置过程比较简单，这里省略。西校区路由器 IPSEC VPN 配置关建代码如下：

```
acl number 3002   //定义访问控制列表，配置 ipsec 感兴趣流
rule 5 permit ip source 192.168.137.0   0.0.0.255 destination 198.168.1.0   0.0.0.255
ipsec proposal dx //创建一个安全提议，名字为 dx
ike proposal 1 //创建 ike 提议，编号为 1
encryption-algorithm 3des-cbc //采用 3DES 链式加密
ike peer sxq v2 //创建名为 sxq 的对等体，使用 ike v2 和对方做密钥协商
pre-shared-key simple dfth //预共享密钥
ike-proposal 1 //调用前面配好的密钥协商方法
remote-address 172.18.2.1// ipsec 对等体的 ip 地址
ipsec policy cl 1 isakmp //创建 ipsec 策略  将前面配好的各项参数，关联在一起
security acl 3002
ike-peer sxq
proposal dx
ipsec policy cl //将策略应用到接口上
```

4.4 测试

使用 ping 命令进行连通性测试，表明链路情况良好。

5　总结

在对比及分析常用 VPN 技术优缺点的基础上，为双校区校园网建设提出了一种 IPSec+MPLS+SSL 相融合的方案，该方案综合了 IPSec、MPLS、SSL 技术的优点，经过 eNSP 模拟组网测试，该方案在保证安全的基础上，用户接入方便、灵活，有一定的扩展性，较好地满足了校园网设计需求。

参考文献：

[1]申淑平.VPN 技术在校园网络安全体系中的应用研究[J].信息与电脑 (理论版)，2022，34 (22)：227-229.

[2]邓诗钊.计算机网络信息安全中虚拟专用网络技术的应用[J].信息系统工程，2023 (08)：84-87.

[3]魏洁玲，马秀丽，金彦亮，等.基于 VPN 通道下的加密流量分类算法[J].应用科学学报，2023，41 (04)：646-656.

[4]刘永辉.计算机网络信息安全中虚拟专用网络技术的运用[J].科技资讯，2023，21 (15)：20-23.

[5]王文飞.VPN 技术在高职院校校园网应用案例浅析[J].科技风，2023 (18)：64-66.

[6]李鑫，张琴.基于多 VPN 技术的高校数字化校园网组建研究[J].山西大同大学学报 (自然科学版)，2017，33 (03)：10-15.