虚拟专用网VPN应用于湖北省烟草企业办公的实践与探索

徐钟晨[1]，曹丽君[2]，郭 利[2]

（1. 湖北省襄阳市烟草公司保康县烟叶分公司，湖北 保康 441600；2. 湖北省烟草公司襄阳市公司，湖北 襄阳 441000）

摘要：虚拟专用网（VPN）是在企业规模逐渐扩大，远程用户、远程办公人员、分支机构、合作伙伴不断增多，关键业务需求增加的前提下，出现的一种通过公共网络（如Internet）来建立自己的专用网络的技术。该网络正应用于湖北省烟草商业系统。从系统实施的背景出发，在分析VPN基本概念的基础上，结合实际情况，从VPN的类型、安全性、功能、应用范围及存在的问题几个方面对该系统进行探索，为该系统改进及应用提供参考。

关键词：VPN应用；类型；安全性；功能

中图分类号：TP393 **文献标识码：**A **文章编号：**1001-1463(2016)01-0069-05

doi:10.3969/j.issn.1001-1463.2016.01.023

随着企业规模逐渐扩大，远程用户、远程办公人员、分支机构、合作伙伴不断增多，关键业务的需求增加，出现了一种通过公共网络（如Internet）来建立自己的专用网络技术，这种技术就是虚拟专用网（VPN）。湖北省烟草商业系统已经开始应用 VPN。VPN 可以实现不同网络的组件和资源之间的相互连接，能够利用 Internet 或其他公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。我们结合 VPN 应用于湖北省烟草企业的实际情况，对该系统进行探索，旨在为该系统改进及应用提供参考。

1 系统实施的背景

随着 Internet 的商业化，大量的企业（如银行、铁路、公司等）规模逐渐扩大，分支机构、合作伙伴也在不断增多，关键业务的需求增加，以及内部网络与 Internet 互连，使现代企业网的概念发生了根本性的变化[1]。同时也给企业及用户带来了一些问题，如公共网上信息在传输中可能泄密、信息在传输中可能失真、信息的来源可能被伪造等信息安全出问题，以及信息在传输中可能成本很高。

目前大、中、小型企业通过公共网络（如 Internet）来建立自己的专用网络的技术就是 VPN。VPN 集灵活性、安全性、经济性、可管理性以及扩展性于一身，可充分满足分支机构、移动办公安全通信的需求。是企业网在因特网等公共网络上的延伸，通过一条私有的通道创建一条安全的私有链接，将远程用户、公司的分支机构、公司的业务伙伴等跟企业网连接起来，形成一个扩展

收稿日期：2015-12-04

作者简介：徐钟晨（1989—），男，湖北武汉人，主要从事计算机通信方面技术研究工作。E-mail：308458926@qq.com

通讯作者：郭 利（1973—），男，湖北襄阳人，高级农艺师，主要从事烟草技术研发和推广工作。E-mail：xfguoli@163.com

的技术优势，利用现代生物技术选育优良品种进行快繁。二要充分调动农民种植积极性与涉农企业投资热情，加强加工技术研究，提高蕤核的产品附加值，使得蕤核制品在能满足国内需求的同时，增强国际竞争力。

参考文献：

[1] 石绍玲. 蕤核的经济价值及育苗技术[J]. 现代农业科技，2013(18)：101.

[2] 杨福红，赵晓明，赵海燕，等. 蕤核的研究进展[J]. 山西农业科学 2008，36(9)：94-96.

[3] 王艺苗，邰源临，张 强，等. 蕤核叶片化学成分的研究[J]. 中国野生植物资源，2012，31(5)：44-48.

[4] 杨丽娟，李相林，李开华. 东北扁核木引种培育技术[J]. 中国林副特产，2008，96(5)：67-68.

[5] 任宪威. 树木学（北方本）[M]. 北京：中国林业出版社，1997.

[6] 黄祥童. 东北扁核木[J]. 特种经济动植物，1998(1)：47.

（本文责编：陈 伟）

的公司企业网。虚拟专用网络是一个提供高安全性能、低价位的因特网接入解决方案。

湖北省烟草商业系统主要承担卷烟销售、烟草专卖打假、烟叶生产与调拨、烟用物资及其他相关的生产经营任务。随着企业的发展，企业信息化建设工作也不断推进，并取得一定效果。为进一步加快企业各类信息的收集及统计，资源共享、提高员工的工作效率，提高数据传输安全性等成为当务之急。为完善企业信息化建设，已初步开始应用 VPN。

2 VPN 的基本概念

VPN 的基本思想是在公共网络上建立安全的专用网络，传输内部信息，形成逻辑网络，从而为企业用户提供比专线价格更低廉、安全性更高的资源共享和互联服务。VPN 是企业内部网的扩展。

VPN 指的是在公用网络上建立专用网络的技术，即通过对网络数据的封包和加密传输，在公用网络上传输私有数据，形成一种逻辑上的专用网络[2]。它向用户提供一般专用网络所具有的功能，但本身却不是一个独立的物理网络。

“虚拟”(Virtual)说明它是一种仿真物理连接的逻辑网络连接，没有固定的物理连接，利用的是公共网络资源。在虚拟专用网中，任意 2 个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是利用公用网络资源（如 Internet、ATM 网络、帧中继网络等）动态组成的。“专用”(Private，或译为“私用”)说明它在功能上等同于传统的专用网络，具有与内部网络相同的安全性、易管理性和稳定性，可被当作专用网络使用。

VPN 至少应能提供如下功能：加密数据[3]，以保证通过公网传输的信息即使被他人截获也不会泄露；信息认证和身份认证，保证信息的完整性、合法性，并能鉴别用户的身份；提供访问控制，不同的用户有不同的访问权限。

3 VPN 的类型

VPN 既是一种组网技术，又是一种网络安全技术。VPN 涉及的技术和概念比较多，应用的形式也很丰富，其分类方式也很多。

3.1 按照应用范围划分

大致可以划分为远程接入虚拟网(Accesss VPN)、企业内部虚拟网(Intranet VPN)和企业扩展虚拟网（Extranet VPN)3种应用模式。Accesss VPN 用于实现移动用户或远程办公室安全访问企业网络；Intranet VPN 用于组建跨地区的企业内部互联网络，湖北烟草商业系统目前正开始使用该类型；Extranet VPN 用于企业与客户、合作伙伴之间建立互联网络。

3.2 按照网络结构划分

一是基于 VPN 的远程访问，是即单机连接到网络，又称点到站点，桌面到网络。用于提供远程移动用户对公司内部网的安全访问。二是基于 VPN 的网络互联，即网络连接到网络，又称站点到站点，网关(路由器)到网关(路由器)或网络到网络。用于企业总部网络和分支机构网络的内部主机之间的安全通信时，还可用于企业的内部网与企业合作伙伴网络之间的信息交流，并提供一定程度的安全保护，防止对内部信息的非法访问。三是基于 VPN 的点对点通信，即单机到单机，又称端对端，用于企业内部网的两台主机之间的安全通信。

3.3 按照接入方式划分

在 Internet 上组建 VPN，用户计算机或网络需要建立到 ISP 的连接。与用户上网接入方式相似，根据连接方式，可分为 2 种类型：①专线 VPN 通过固定的线路连接到 ISP，如 DDN、帧中继等都是专线连接；②拨号接入 VPN 简称 VPDN，使用拨号(如模拟电话、ADSL 等)连接到 ISP，是典型的按需连接方式，这是一种非固定线路的 VPN。

4 VPN 的安全性

随着网络规模的扩大，网络应用业务的增长，企业内部网的安全越来越受重视，机构之间、部门之间需要在一些关键的应用系统之间进行隔离，实现访问控制。用于 Internet 的 VPN 技术也同样适用于 Intranet，VPN 可用于任何广域网或局域网环境中，在内部网中实现安全保密通信，建立内部专用隧道，从而组建更为专用的保密网络或者秘密网络。VPN 采用隧道技术向用户提供无缝、安全、端到端的链接服务，以确保信息资源的安全。

为了实现业务网络隔离，通常在企业局域网中使用 VLAN 技术，防止无关人员对特定信息的访问。然而，VLAN 并不是完善的安全解决方案，

不能实现数据加密，如果再使用 VPN 加以改造，就可实现更安全的网络隔离。如企业内部 2 个承担关键业务的部门，如财务部门和总经理办公室之间，可设置自己的逻辑专用网，通过 VPN 方式来连接，他们之间穿过企业网的通信是加密的，其他部门的人员无法获取。在这种 VPN 结构中，数据采用复杂的算法来加密传输信息，使得数据不会被窃取，这种算法在公网中通过多层虚拟通道从 VPN 设备的一端到达另一端。隧道从一个 VPN 设备开始，通过路由器横跨整个 Internet 到达其它 VPN 设备，并以数字证书来标记整个隧道，以此来鉴别属于此 VPN 的隧道。隧道的第 2 层是数据的封装包，到达目标 VPN 设备的是重新分装后的数据。隧道的第 3 层是身份验证，采用不同的算法来验证信息来源的真实性[4]。隧道的最里层就是加密，来确保信息的机密性。

VPN 使数据通过高强度的加密算法进行传输，确保数据传输具备防窃听、防篡改特性；有安全可靠的身份认证机制保证接入用户的合法性。同时，实现管理员对服务器的远程维护、数据的完整性、网络设备及安全设备的远程维护等问题，设置了权限管理功能、以及根据不同的用户、设置了不同的访问权限。

许多行业用户，如银行、政府等，都建立了自己的专用广域网，随着网络业务种类的加多，需要解决内部网本身的安全问题，在一些关键的应用系统之间实现隔离，进行访问控制。使用 VPN 技术即可达到该目的，在同一个物理广域网上实现不同业务的逻辑网络隔离，不必为每一个业务网建设独立的物理网络，从而简化了总体成本和维护工作。

5 VPN 的功能

基于虚拟专用网络的安全性，为了保障数据安全传输，可将 VPN 功能分为：数据机密性保护功能、数据完整性保护功能、数据源身份认证、重放攻击保护。

5.1 数据机密性保护

VPN 可限制数据游走的方向，实现数据流控制。同时，对数据应用了加解密技术，根据不同主体之间的差异对数据进行自动加解密，当用户、进程等获得授权的主体访问目标数据时，加密数据将自动转换成明文，而非授权主体访问时加密数据的呈现内容则为密文，因此，即使攻击者获得受保护的数据，也无法读取和使用。

5.2 数据完整性保护

VPN 可对内部子网发送的数据包进行 hash 提取摘要，同时对原始数据包进行加密后发送。客户端接收到原始数据包后对其进行机密，并对接收的数据包进行 hash 提取摘要与原发送的摘要进行比较，验证数据的完整性。

5.3 数据源身份认证

主要可分为 4 步：①客户机向 VPN 服务器发出连接请求；②VPN 服务器响应请求并向客户机发出身份认证的请求，客户机与 VPN 服务器通过信息的交换确认对方的身份，这种身份确认是双向的；③VPN 服务器与客户机在确认身份的前提下开始协商安全隧道以及相应的安全参数，形成安全隧道；④ VPN 服务器将在身份验证过程中产生的客户机和服务器公有密钥用来对数据进行加密，然后通过 VPN 隧道技术进行封装、加密，传输到目的内部网络。

目前湖北烟草商业系统主要采用 USB key 技术及数字签名技术。USB key 是一种 USB 接口的秘密数据存储设备，具有硬件 PIN 码保护功能。每一个 USB Key 都具有硬件 PIN 码保护，PIN 码和硬件构成了用户使用 USB Key 的 2 个必要因素，即所谓“双因子认证”。用户只有同时取得了 USB Key 和用户 PIN 码，才可以登录网上银行系统。即使用户的 PIN 码被泄漏，只要用户持有的 USB Key 不被盗取，合法用户的身份就不会被仿冒；如果用户的 USB Key 遗失，拾到者由于不知道用户 PIN 码，也无法仿冒合法用户的身份。USB Key 具有 8 ~ 64 K 的安全数据存储空间，可以存储数字证书、用户密钥等秘密数据，对该存储空间的读写操作必须通过程序实现，用户无法直接读取，其中用户私钥是不可导出的，杜绝了复制用户数字证书或身份信息的可能性。USB Key 内置 CPU 或智能卡芯片，可以实现 PKI 体系中使用的数据摘要、数据加解密和签名的各种算法，加解密运算在 USB Key 内进行，保证了用户密钥不会出现在计算机内存中，从而杜绝了用户密钥被黑客截取的可能性。

数字签名技术主要用于保护被签名信息的真

实性和完整性。同时也隐含了对信息发送方的身份认证功能。对于中心式的认证机制，以证书认证技术为例说明。基于数字证书认证技术的认证是通过证书认证中心发放数字证书来进行用户身份认证的[1]。数字证书的作用在于证明证书所包含的密钥属于证书所有人，因此一个很明显的问题是需要对所有需要进行认证的实体进行全球范围内唯一的命名。现行的命名体制是一种层级式的机制。证书使用过程中，应用需要确定密钥执有者是否有权限访问特定资源，因此需要在证书中携带授权信息。

证书的申请过程大致是：用户将自己生成/得到的公钥提交给 CA，由 CA 将该公钥、该用户的本地命名、该 CA 的标识以及有效性条件等选项共同使用该 CA 的私钥签名后生成数字证书发给用户。对于发布的证书，CA 将同时在本地的 X1500 目录服务中予以记载，供用户查找使用。

证书认证的基本过程是：用户将证书提交给应用，应用首先查看发布证书的 CA，若应用不信任该 CA，则首先需要对该 CA 的身份进行验证，即向该 CA 的上一级 CA 请求验证，若对上一级 CA 仍不信任，则需要递归向上请求验证，直到查找到应用信任的 CA 或 RootCA 为止。确认发布证书的 CA 身份后，再向该 CA 查询目录服务，确信该证书由该 CA 发布，并检查 CRL 确认证书的有效性，然后再使用该 CA 的公钥对证书的 CA 签名进行验证后才接受该证书[5-6]。

5.4 重放攻击保护

VPN 中使用了 ESP 封装协议，该协议能够抵御重放攻击，见图 1。

一个 32Bt 的字段，用来标识处理数据包的 SA。SPI 是明文发送的，用来告知对方路由器。SA 建立之初，序列号初始化为 0，使用该 SA 传递的第一个数据包为零，每收到一个数据包，序列号就会 +1，如果再次收到相同的则放弃。主要用来防重放攻击。

6 VPN 的应用范围

VPN 主要用作远程访问和网络互联的廉价、安全、可靠的解决方案；帮助远程用户、公司分支机构、商业伙伴及供应商同企业内部网建立可信的安全连接，并保证数据的安全传输。VPN 既

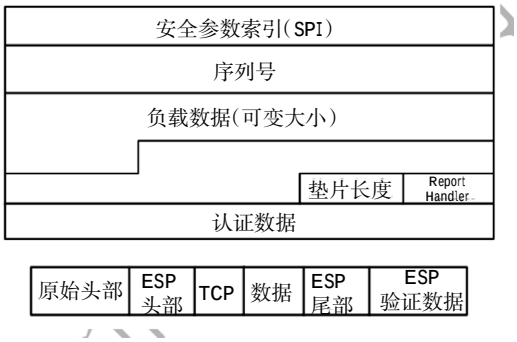

图 1 VPN 中 ESP 封装协议

是一种组网技术，又是一种网络安全技术。遇到以下几种情况，可考虑选择 VPN：①已经通过专线连接实现广域网的企业，由于增加业务，带宽已不能满足业务需要，需要经济可靠的升级方案；②企业的用户和分支机构分布范围广、距离远，需要扩展企业网，实现远程访问和局域网互联，最典型的是跨国企业、跨地区企业；③分支机构、远程用户、合作伙伴多的企业，需要扩展企业网，实现远程访问和局域网互联；④关键业务多且对通信线路保密和可用性要求高的用户，如银行、证券公司、保险公司等。

目前，像金融证券、保险业和政府机关等一类的行业用户，还有一些跨国企业、跨地区企业和分支机构分散的企业或机构，采用 VPN 技术的比较多。随着业务信息化程度的提高，中小企业应用 VPN 的要求也更加强烈。

7 VPN 存在的问题

在日常工作中对系统中的应用与探索，还存在一些问题：①VPN 稳定性不够，在使用过程中不定时会出现虚拟网络连接掉线重连；②VPN 速度不够，在使用内部网络传输下载文件时，经常出现传输速率较慢现象。

8 结语

VPN 技术不仅会大大节省企业网的建设和运行维护费用，而且增强了网络的可靠性和安全性，满足信息系统安全等级保护要求，VPN 技术和产品对推动信息系统安全等级保护建设将起到不可低估的作用。

参考文献：

[1] 黄 聪. Citrix 平台+SSL VPN 应用于远程办公的实践初探[J]. 科技资讯，2008(10)：93.
[2] 蒋东毅，吕述望，罗晓广. VPN 的关键技术分析[J]. 计算机工程与应用，2003(15)：173-177.

林芝市八一镇近郊观光采摘旅游现状及发展策略

王忠斌，王建宇
（西藏大学农牧学院资源与环境学院，西藏 林芝 860000）

摘要：在调查八一镇周边区域观光采摘资源现状的基础上，探讨了该区域发展休闲观光采摘旅游存在的问题，进而提出了科学合理的对策。

关键词：八一镇；观光采摘旅游；对策
中图分类号：F592 **文献标识码：**A **文章编号：**1001-1463(2016)01-0073-03
doi:10.3969/j.issn.1001-1463.2016.01.024

观光采摘旅游是近年来随着生活水平的提高、城市化程度的加快、人们环境意识的增强以及农村经济的发展，而逐渐出现的集观光、采摘、旅游、休闲度假于一体，经济效益、生态效益和社会效益相结合的综合性旅游产品，旅游者通过亲自参与果蔬采摘过程来获得收获的乐趣，放松身心。作为一种新兴的体验型旅游休闲方式，观光采摘旅游的发展不仅可以满足旅游者渴望回归自然、亲近自然的需求，而且也可成为现代新型农业的一个新的经济增长点，有效地促进了农村经济的快速发展[1-4]。

八一镇位于西藏东南部的林芝地区林芝县，北纬 29° 50′，东经 93° 25′，海拔 2 900 m，总面积为 5 km^2，总人口 3.8 万，是林芝市的政治、经济、文化中心。八一镇位于尼洋河畔，距雅鲁藏布江与尼洋河交汇处 30 km，地处平坦的河谷地带，受印度洋暖湿气流的影响，该区域气候温暖湿润，降雨充沛，年降雨量 650 mm 左右，水资源较为丰富；年均温度 8.7 ℃，年均日照 2 000 h，无霜期 180 d，高原昼夜温差大，光合作用效率高，为果蔬种植提供了优越的气候条件。我们在调查八一镇周边区域观光采摘资源现状的基础上，探讨了该区域发展休闲观光采摘旅游存在的问题，进而提出了科学合理的发展策略，以期为加快八一镇近郊观光采摘旅游经济的发展提供参考。

1 现状

八一镇近郊的果蔬种植地数量众多，呈分散性分布，大多为外地人所承包，主要种植草莓、西瓜等时令蔬菜瓜果。每当瓜果成熟的季节，部分八一镇居民会自驾到农场、果园进行采摘活动。

林芝县观光采摘旅游资源相对来说比较单一，现有的观光采摘旅游资源仅有八一镇巴吉村、章巴草莓村及米林嘎玛农场。巴吉村有 30 个大棚，面积 9 990 m^3；章巴村有 40 个大棚，面积 13 320 m^3，均以种草莓为主。米林嘎玛农场全场土地分布于米林、林芝两县，总面积 656.6 hm^2，其中耕地面积 375.2 hm^2、果园面积 243.88 hm^2、牧地面积 37.52 hm^2，目前已发展成为西藏最大的水果产业基地、苗木繁育基地以及无公害禽蛋、肉鸡生产供应基地。其中果园水果品种多样，主要种植葡萄、苹果、油桃、梨、西瓜、草莓、西红柿、李子、樱桃等高原水果(表1)。

2 存在的问题

2.1 未形成产业模式

八一镇的观光采摘旅游是近几年慢慢兴起的，尚处于起步阶段，还未真正形成产业模式，处于摸索时期。

收稿日期：2015-11-26
作者简介：王忠斌(1983—)，男，宁夏彭阳人，讲师，硕士，主要从事区域旅游规划与开发工作。联系电话：(0)13889049430。E-mail：0823yuan1020@163.com

[3] 查振兴，王 振. VPN 在信息系统安全等级保护中的应用[J]. 电子世界，2013(19)：71.
[4] 江 红，余青松，顾君忠. VPN 安全技术的研究与分析[J]. 计算机工程，2002(4)：130-132.
[5] 翁 亮，陈依群，诸鸿文. VPN 用户认证技术[J]. 通信技术，1999(4)：47-51.
[6] 冯栋梁. 浅谈 SSL VPN 的十种认证方式[J]. 科技与创新，2015(5)：79.

(责任编辑：张杨林)