文章编号:1000 - 582X(2002)04 - 0032 - 04

基于 IP - VPN 的协同设计网络安全问题*

付红桥，何玉林，先志玲，王旭霞
（重庆大学 机械工程学院，重庆 400044）

摘　要:异地协同设计与制造技术作为敏捷制造的重要方法和手段，已经成为制造业研究的热点。介绍了 IP - VPN 的基本概念和关键技术，提出了一个基于 IP - VPN 的实用协同设计网络模型。而异地协同设计是典型的多用户参与的多任务系统，用户之间存在大量的协同过程，因此网络平台的安全性是协同设计实施的关键问题。对基于 IP - VPN 的协同设计网络的安全性问题进行了研究，得出了通过采用数据加密、用户认证和基于角色的多层强制访问控制等技术可以构建一个经济、实用、安全的协同设计网络平台的结论。

关键词:IP - VPN 协同设计网络;认证;加密
中图分类号:TP391.4　　**文献标识码**:A

异地协同设计与制造技术作为敏捷制造的重要方法和手段，已经成为制造业研究的热点。为了实现异地协同设计与制造，一个经济、实用、安全、跨平台的协同设计网络平台的建立具有重要的意义，而网络平台的安全性是网络能否实用的重要标准。笔者研究了基于 IP - VPN 的协同设计网络的安全性问题，提出了一个经济、实用、安全的协同设计网络模型。

1　IP - VPN 的基本概念与特征

虚拟专用网(VPN: Virtual Private Network)指的是在公用网络上建立专用网络的技术。称为虚拟网主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台(如 Internet, ATM, Frame Relay 等)之上的逻辑网络，用户数据在逻辑链路中传输[1]。

VPN 的功能就是保证建立在公共网络上的企业网络安全地传递信息，它有着与私有网相同的策略。可以在 IP、帧中继、ATM 或 Internet 上建立 VPN。它具有同客户原有的私有网络相同的安全性、优先级特性、易管理性和稳定性。它可以满足客户对原企业网与 Remote Office、移动用户、远程用户间无缝连接的要求，即将网络连接扩展到客户、供货商、合作者和关键用户以形成 Extranet 来降低商业运作开支和提升服务质量(包括速度、简便性和保密性上的提升)。

IP - VPN(IP Based Virtual Private Networks，基于 IP 的虚拟专用网技术)，就是指利用现有的不安全的公共 IP 网络环境，构建具有安全性、独占性并自成一体的虚拟网络。

IP - VPN 的概念揭示了 IP - VPN 的 4 个本质特征[2]：

1) 基于公共的 IP 网络环境：这是在 VPN 前冠以 IP 的根本原因。由于像 Internet 这样的 IP 网络环境构建在诸多的 TCP/IP 标准协议簇之上，有着工业界最广泛的支持，所以，使得利用 IP - VPN 技术组网，经济、便利、可靠、可用，同时组网灵活，具有良好的适应性和可扩展性。

2) 安全性：由于是构建在像 Internet 这样的公用 IP 网络环境之上，所以要采用网络安全技术，来保证网络信息的机密性、完整性、可鉴别性和可用性，这样才能达到 IP - VPN 的“专用”，这也是 IP - VPN 的关键所在。

3) 独占性：这是用户对构建在公用网络上的 IP - VPN 的一种感觉，其实是在与其他用户或其他企业共享公用网络。

4) 自成一体：IP - VPN 同专用网一样，自成一体，

* **收稿日期**:2001 - 11 - 30
基金项目:黑龙江省重点 CAD 应用工程项目“家具计算机辅助设计系统”
作者简介:付红桥(1968 -)，男，湖北罗田人，重庆大学博士研究生，工程师。主要研究方向：CIMS、IQS、网络化协同设计。

可以拥有自己的地址空间，可以使用非 IP 协议如 IPX 等。换句话说：IP－VPN 具有网络地址翻译（NAT）和多协议支持的能力。

因此，安全性、独占性及自成一体的自主性使得构建在公用 IP 网络环境上的 IP－VPN 能够做到“虚拟、专用”。

2　IP－VPN 的隧道技术

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式，它利用一种网络传输协议，将其他协议产生的数据报文封装在它自己的报文中，在网络中传输。IP 隧道代替了传统 WAN 互联的“专线”，是组建“虚拟网络”的基础。

2.1　IP 隧道的“封装”机制

“封装”是构建隧道的基本手段，它使得 IP 隧道实现了信息隐蔽和抽象，为 IP－VPN 提供 NAT、多协议支持等机制奠定了基础。图 1 是隧道封装示意图，关于隧道的形成参见文献[3]。

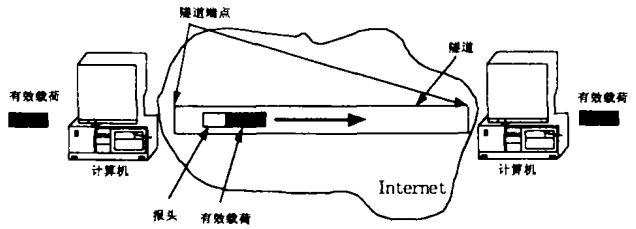

图 1　隧道封装示意图

2.2　IP 隧道的实现机制

IP 隧道的实现机制主要涉及到两个方面：一是隧道所建立的连接是“虚拟”的链路层还是网络层；二是在网络的什么层次上实现 IP 隧道问题。目前一般的做法是用 IP 协议实现 IP 隧道，但也有用 UDP 等协议来实现 IP 隧道的，从实现的细节上来说，还要考虑传输效率、MTU 限制及“碎包”处理和 IP 隧道的状态易于监控和管理等问题。对于 IP 隧道来说，当在隧道的开启处封装及在隧道的终止处还原装配数据包时，进行包的过滤、检查是非常方便的，所以 VPN 网关通过“过滤型”隧道可直接融入“包过滤”防火墙机制，进一步增强了 VPN 的安全性。VPN 网关支持多条隧道，同时管理多个 IP－VPN，是企业组成 Extranet 的需求，它可从管理、加密认证算法、密钥管理等方面综合解决这一问题。

3　基于 IP－VPN 的协同设计网络模型

协同设计网络就是将现有的各种在地理位置上或逻辑上分布的企业或公司，通过 Agent 连接到计算机网络中去，以提高各个企业或公司间的信息交流与合作设计能力，进而实现资源的共享。由于企业或公司的相对独立性，为了到达协同的目的，这就要求协同设计网络具有以下特性：1）开放性；2）跨平台；3）实时性；4）安全性；5）经济性；6）可扩展性；7）灵活性等。

为了满足上述要求，一个协同设计网络应该是基于 Internet 的，但由于 Internet 是一个不可管理的网络，基于 Internet 的企业商务，安全隐患丛生。因此，虚拟专用网（VPN）方案应运而生，为企业提供了较高的安全性，让企业网络延伸到全世界。

下面以某企业为例建立一个协同设计网络模型。假设该企业在某高校有一个合作的远程设计中心，一个分公司，一个合作伙伴，同时该企业还要求满足出差人员和一些零星客户的访问需要。为此，建立了如图 2 所示的网络模型。图中可以看到，公司总部网段配有 VPN 中心，它通过路由器接入 Internet，远程设计中心、合作伙伴、分公司等可以通过 IP VPN 设备或通过拨号接入本地 ISP 的 POP（Point of Presence，接入点）服务器，出差员工（移动用户）和客户可利用 MODEM 通过 PSTN 网连入本地 ISP 的 POP 服务器接入 Internet，这样通过 Internet 即可实现相互通信，从而可以共享资源和协同工作。

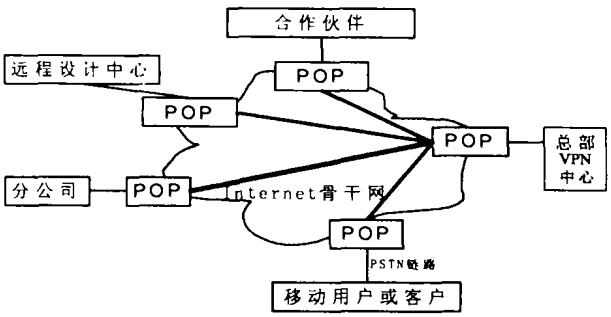

图 2　基于 IP－VPN 的协同设计网络模型

4　基于 IP－VPN 的网络安全性分析

基于 IP－VPN 的协同设计网络的一个重要环节是数据的安全性。IP－VPN 是利用开放性的公用网络作为用户信息传输的媒体，通过附加的隧道封装、信息加密、用户认证和访问控制等技术实现对信息传输过程的安全保护，从而向用户提供类似专用网络的安全性能。

4.1　隧道协议

隧道协议是“专用网络”的保证，目前用于 IP 隧道的有代表性的安全协议是：PPTP、L2F、L2TP、IPSec 等。PPTP 受到了以 Microsoft 为代表的一些厂家的支持，它允许在一个 IP 网上利用虚拟 PPP 连接建立 VPN。

L2TP 则是将 PPTP 与 Cisco 的 L2F 结合而产生的一个新的协议,与 PPTP 十分相似,但支持非 IP 协议如 AppleTalk 和 IPX。IPSec 在 IETF 的指导下由 IETF 的 IP 安全性工作组不断发展和完善而来,它实际上是一个安全协议簇,用于确保网络之间的安全通信。

根据隧道协议,隧道技术让企业能建立逻辑上的点对点网络连接,采用点对点传输技术,可以确保非授权的用户,无法读取到他人的机密文件。

4.2 数据加密

目前存在两种类型的软件加密方法:分享密钥(Shared Key)和公开密钥(Public Key)加密方法。

4.2.1 分享密钥加密方法

分享密钥方法加密和解密密钥是一样的,其加密解密速度非常快,但是密钥的管理比较困难,它必须使信息的发送者和接收者都明确同一个密钥,通常还需要其它的更安全的信道来传送密钥。此外,如果发送者需要与许多人通信时,就要管理许多的密钥。

较著名的分享密钥加密是 DES(Data Encryption Standard),它利用 56 位密钥加密 64 位块的正常文本文件;3DES 利用 3 个密钥加密 3 次,但其速度慢得多了。

4.2.2 公开密钥加密方法

加密和解密密钥不是同一个,发送者用接收者的公开密钥加密信息,接收者用自己的私有密钥解密信息。公开密钥加密的优点是容易管理密钥,不需要发送者和接收者都明确同一个密钥(分享密钥),需要保密的私有密钥保存在其所有者处等;其弱点是数学计算比较复杂,加密和解密速度慢,并且需要注册有效的公开密钥箱(public component)。最流行的例子为 RSA。

数据加密是任何 VPN 设备的基本要求,而各种 VPN 设备的一个主要不同点在于采用加密算法和密钥的强度不同。加密是一项复杂的处理过程,特别是网络中有大量的信息传输时,CPU 要承担大量的计算负担。因此,目前 VPN 市场趋向于采用更安全、处理速度更快的专用硬件设备,这更适合于采用较长位数加密算法,数据加密则保证敏感数据不会被盗取,有利于提高安全性能和适用于未来通信发展的需要。

4.3 密钥管理

由于加密算法是公开的,所以加密过程的强度就取决于如何使用密钥来加密和解密被传输的数据以及密钥管理所使用的协议。密钥交换必须采用很强的基于密钥管理标准的算法。目前 VPN 技术加密的首选标准是 IKE 协议,它能适应不同的加密密钥。

4.4 用户认证

用户认证是 VPN 设备的注册和鉴别过程。它要求各个 VPN 设备与 CA(认证中心)建立秘密的连接和确认。用户认证确保未获认证的用户无法访问网络。

目前采用的认证技术按照实现过程中是否需要专门的外部管理中心可分为分布式认证技术和中心式的认证技术。分布式认证技术主要利用数字签名技术进行分布式验证,而中心式的认证技术包括 Kerberos 认证技术以及基于数字证书的认证技术,由中心发放一定的证书或票证以证明用户的身份。这两类认证技术在 VPN 中的应用文献[4]进行了细致的研究和分析,为 VPN 用户认证技术的实现提供了技术框架。

4.5 基于角色的多层强制访问控制[5]

一个完善的 VPN 系统不仅要采用加密技术,而且有高效的访问控制(如防火墙),采用基于角色的强制访问控制技术,既可以保证协同设计人员具有相应的权限,进行相应的工作,同时又保证了数据的安全,对未授权用户或黑客有很好的防御作用。

4.6 网管的安全

VPN 系统的网管信息是网络中最敏感的信息,其中包括安全规则表更新、安全审计、日志数据、密钥交换参数定义、加密和验证方法等重要信息。为了维护这些机密信息,VPN 系统也采用同样的加密技术来加密这些信息。更安全的方法是采用专用的加密防火墙系统来保护中央网管工作站。这实际上不仅保护了网管信息在公网上传输的安全性,而且把 VPN 系统管理员同网络的其他本地用户隔离开来,避免了内部用户破坏 VPN 系统的安全。

随着宽带技术的发展,VPN 已经建立在 IP 宽带网上[6],通过采用一些先进技术,对于保证 IP - VNP 应用的网络扩展性、安全性和可管理性都有重要的意义。

5 结 论

通过对协同设计网络模型的安全性的分析可以知道,基于 IP - VPN 的协同设计网络是完全可以依赖的安全网络,同时由于 VPN 具有成本低、访问费用低、可扩展性好、安装简便、易于管理等特性,因此基于 IP - VPN 的协同设计网络模型对于企业的异地协同设计具有重要的实用意义和经济价值。

参考文献:

[1] 仲翼 . 虚拟专用网(VPN)实现公网专用[EB/OL]. 赛迪网 http://www.ccidnet.com/,2001 - 11 - 02/2001 - 11 - 30.

[2] 陈性元,宋国文 .IP - VPN 及其关键技术[J]. 电信科学,2000,(5):38 - 42.

[3] 辛明君,李洪,夏小明 .VPN 技术综述(上)[J]. 电信技术,

2000,(4):12－15.
[4] 翁亮,陈依群,诸鸿文[J].VPN 用户认证技术．通讯技术,1999,(4):47－51.
[5] 哈进兵,张友良．一种异地协同设计中的安全策略[J].工程设计,2001,(4):17－20.
[6] 施一萍,白英采．IP 宽带网中基于 MPLS 技术的 VPN 应用[J].计算机应用和软件,2001,18(7):1－3.

Research on Cooperative Design Network Security Based on IP-VPN

FU Hong-qiao, HE Yu-lin, XIAN Zhi-ling, WANG Xu-xia
(College of Mechanical Engineering, Chongqing University, Chongqing 400044, China)

Abstract: As the important method and instrument of agile manufacture, the technology of distributed collaborative design and manufacturing has become the hotspot of manufacturing. The basic concept and key technologies of IP-VPN are introduced in this paper, and a collaborative design network model based on IP-VPN is presented. Distributed collaborative design is a multi-user, multitask involved system, which is consisted of lots of collaborative processs, so the network security is the key of distributed collaborative design. We research on the security of collaborative design network based on IP-VPN, hence get a conclusion: we can construct an economical、practical and secure collaborative design network system by the application of data encryption, user authentication and access control based on the role, etc.

Key words: IP based Virtual Private Network(IP-VPN); collaborative design network; authentication; encryption; access control

(责任编辑　张小强)

(上接第 31 页)

Solid Model Design on the Features of Products

LI Shao-bin
(Department Of Art Design, Chongqing Normal University, Chongqing 400047, China)

Abstract: To research the problem of plastic art design and emulation of products with the virtual reality technology can short the product development cycle and reduce the cost. This paper discusses the information based on the product feature , solid model with parameters, the structure and function of this system. Combined the product properties with its solid model. Proposed a method with CAD to create the model of the product based on features in the product design. Expressed its feature parameter and shape of model fully . In the case for a deceleration box the feature model has solved the problem of physical information , geometry information and the informative process in its production management system efficiently.

Key words: feature model; parameter design; solid model

(责任编辑　成孝义)