

VPN 中的隧道技术研究

程 思^{1,2},程家兴³

(1. 安徽大学 计算机科学与技术学院,安徽 合肥 230039;

2. 安徽医科大学 计算中心,安徽 合肥 230000;

3. 安徽大学 计算智能与信号处理教育部重点实验室,安徽 合肥 230039)

摘 要:大规模的组建 VPN 网络已经成为一种趋势,越来越多地受到用户的广泛关注。从总体来说,VPN 技术非常复杂,它涉及到通信技术、密码技术和现代认证技术,是一项交叉科学。隧道技术对于构建 VPN 来说,是一个关键性技术。它在源局域网与公网的接口处,将数据作为负载封装在一种可以在公网上传输的数据格式中,在目的局域网与公网的接口处将数据解封装,取出负载。从隧道技术的发展,对各种隧道技术做了一个简单的分析,了解 VPN 组网的安全技术。

关键词:VPN;隧道技术;安全

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2010)02-0156-04

A Brief Discussion on Tunnel Technical of VPN

CHENG Si^{1,2},CHENG Jia-xing³

(1. School of Computer Science and Technology in Anhui University, Hefei 230039, China;

2. Computer Center in Anhui Medical University, Hefei 230000, China;

3. Ministry of Edu. Key Lab. of Intelligent Computing & Signal Processing, Anhui Univ., Hefei 230039, China)

Abstract:Setting-up large-scale VPN network becomes an important task, VPN has been attracted extensive attention of business subscribers. In one speak, VPN technology is very complicated, it involves in communication technology, cryptography, authentication technology, it is an interdisciplinary. Tunnel technology is a key technology to set-up VPN network. In the port of host LAN and Internet, the data is packed in a pattern that can transport in Internet, in object LAN, the data is decompression and can use it. Give a simple analysis of the tunnel technique from the development of tunnel technique, to know the security technical of the setting-up large-scale VPN.

Key words:VPN; tunnel technical; security

0 引言

随着网络技术的飞速发展,各企业或高等学校内部的信息交换日益频繁,企业的分支机构也越来越多。但是,这样的信息交流不但带来了网络的复杂性,还带来了管理和安全性的问题,因为 Internet 是一个全球性和开放性的、基于 TCP/IP 技术的、不可管理的国际互联网络^[1],因此,基于 Internet 的商务活动就面临非善意的信息威胁和安全隐患。因此,用户的信息技术部门在连接分支机构方面也感到日益棘手。用户的需求正是虚拟专用网技术诞生的直接原因。

1 VPN 涵义

为了使得远程的企业员工可以与总部实时的交换数据信息,企业得向 ISP 租用网络提供服务。但公用网容易遭受各种安全攻击(比如拒绝服务攻击来堵塞正常的网络服务,或窃取重要的企业内部信息)。

VPN 这个概念的引进就是用来解决这个问题。它是利用公用网络来连接到企业私有网络。但在 VPN 中,用安全机制来保障机密性,真实可靠性,完整性严格的访问控制。这样就建立了一个逻辑上虚拟的私有网络。虚拟局域网提供了一个经济有效的手段来解决通过公用网络安全地交换私有信息。

2 VPN 的基本要求

一般来说,企业在选用一种远程网络互联方案时都希望能够对访问企业资源和信息的要求加以控制,所选用的方案应当既能够实现授权用户与企业局域网

收稿日期:2009-06-03;修回日期:2009-09-05

基金项目:教育部博士点基金(200403057002)

作者简介:程 思(1982-),女,安徽怀宁人,硕士研究生,研究方向为 VPN 技术、VPN 组网技术;程家兴,教授,博士生导师,研究方向为智能计算、算法分析及最优化方法。

资源的自由连接,不同分支机构之间的资源共享;又能确保企业数据在公共互联网络或企业内部网络上传输时安全性不受破坏。因此,最低限度,一个成功的VPN方案应当能够满足以下所有方面的要求:

(1)用户验证。

VPN方案必须能够验证用户身份并严格控制只有授权用户才能访问VPN。另外,方案还必须能够提供审计和计费功能,显示何人在何时访问了何种信息。

(2)地址管理。

VPN方案必须能够为用户分配专用网络上的地址并确保地址的安全性。

(3)数据加密。

对通过公共互联网络传递的数据必须经过加密,确保网络其他未授权的用户无法读取该信息。

(4)密钥管理。

VPN方案必须能够生成并更新客户端和服务器的加密密钥。

(5)多协议支持。

VPN方案必须支持公共互联网络上普遍使用的基本协议^[2],包括IP、IPX等。以点对点隧道协议(PPTP)或第2层隧道协议(L2TP)为基础的VPN方案既能够满足以上所有的基本要求,又能够充分利用遍及世界各地的Internet互联网络的优势。其它方案,包括安全IP协议(IPSec),虽然不能满足上述全部要求,但是仍然适用于在特定的环境。

3 VPN安全技术

由于传输的是私有信息,VPN用户对数据的安全性都比较关心。

目前VPN主要采用四项技术来保证安全^[3],这四项技术分别是隧道技术(Tunneling)、加解密技术(Encryption & Decryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication)。

隧道技术是VPN的基本技术,类似于点对点连接技术,它在公用网建立一条数据通道(隧道),让数据包通过这条隧道传输。加解密技术是数据通信中一项较成熟的技术,VPN可直接利用现有技术。密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为SKIP与ISAKMP/OAKLEY两种^[3]。SKIP主要是利用Diffie-Hellman的演算法则,在网络上传输密钥;在ISAKMP中,双方都有两把密钥,分别用于公用、私用。身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

4 隧道技术

隧道技术是一种利用公共网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据可以是使用不同协议封装的数据包,隧道协议将这些其他协议封装的数据包重新加密并封装在新的包头中发送。新的包头提供了路由信息,从而使新封装的数据包能够在隧道的两个端点之间通过公共互联网络进行路由传输^[3]。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点,数据将被解包并转发到最终目的地。隧道中数据的传输过程如图1所示。

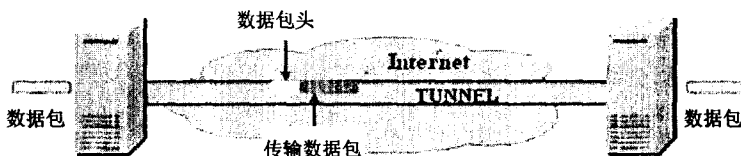


图1 隧道中数据传输过程

隧道所使用的传输网络可以是任何类型的公共互联网络,文中主要以目前普遍使用的Internet为例进行说明。此外,在企业网络同样可以创建隧道。

4.1 第二层隧道协议

第二层隧道协议是先把各种网络协议封装到PPP中,再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。创建隧道的过程类似于在双方之间建立会话;隧道的两个端点必须同意创建隧道并协商隧道各种配置变量,如地址分配,加密或压缩等参数。第二层隧道协议有L2F、PPTP、L2TP等。

4.1.1 点对点隧道协议(PPTP)

PPTP将PPP数据帧封装在IP数据报内通过IP网络,如Internet传送。PPTP还可用于专用局域网络之间的连接。PPTP使用一个TCP连接对隧道进行维护,使用通用路由封装(GRE)技术把数据封装成PPP数据帧通过隧道传送。可以对封装PPP帧中的负载数据进行加密或压缩。

4.1.2 第2层转发(L2F)

L2F是Cisco公司提出的隧道技术,作为一种传输协议L2F支持拨号接入服务器将拨号数据流封装在PPP帧内通过广域网链路传送到L2F服务器(路由器)。L2F服务器把数据包解包之后重新注入(inject)网络。与PPTP和L2TP不同,L2F没有确定的客户方。应当注意L2F只在强制隧道中有效。

4.1.3 第2层隧道协议(L2TP)

L2TP结合了PPTP和L2F协议。设计者希望L2TP能够综合PPTP和L2F的优势。

L2TP是一种网络层协议,支持封装的PPP帧在

IP, X.25, 帧中继或 ATM 等的网络上进行传送。当使用 IP 作为 L2TP 的数据报传输协议时, 可以使用 L2TP 作为 Internet 网络上的隧道协议。L2TP 还可以直接在各种 WAN 媒介上使用而不需要使用 IP 传输层。

4.2 第三层隧道协议

IPSec 是指 IETF (因特网工程任务组) 以 RFC 形式公布的一组安全 IP 协议集, 是为 IP 及其以上协议 (TCP 和 UDP 等) 提供安全保护的安全协议标准。其目标是把安全机制引入 IP 协议, 通过使用密码学方法支持机密性和认证服务等安全服务。IPSec 通过在 IP 协议中增加两个基于密码的安全机制—认证头 (AH) 和封装安全载荷 (ESP) 来支持 IP 数据报的认证、完整性和机密性。

IPSec 协议族包括: IP 安全架构、认证头 AH、封装安全载荷 ESP 和 Internet 密钥交换 (IKE) 等协议。IP 安全架构协议指定了 IPSec 的整个框架, 是 IP 层安全标准协议^[4]。AH 协议定义了数据源认证和完整性验证的应用方法。ESP 为 IP 数据报文提供数据源验证、数据完整性校验、抗重播和数据加密服务。IKE 为 AH 和 ESP 提供密钥交换机制, 在实际进行 IP 通信时, 可以根据实际安全需求, 同时使用 AH 和 ESP 协议, 或选择使用其中的一种。

AH 和 ESP 都可以提供认证服务, AH 提供的认证服务要强于 ESP, 但不对数据报文进行加密, 如图 2 所示。

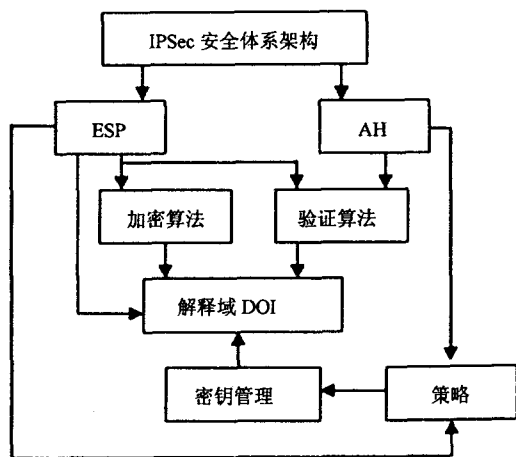


图 2 IPSec 体系结构

IPSec 的安全服务是由通讯双方建立的安全联盟 (SA) 来提供的。SA 为通讯提供了安全协议、模式、算法和应用于单向 IP 流的密钥等安全信息, 这些信息由 SAD 管理提供。当 IP 报文流经 IPSec 设备时, 系统对比安全策略库 (SPD) 中相应的安全策略, 对 IP 报文进行不同的处理。处理方法一般有三种: 丢弃、绕过和

IPSec 保护。如果选择了 IPSec 保护, 根据 SPD 和 SAD 的对应关系, 找到相应的 SA, 进行指定的 IPSec 处理。

4.3 新兴的隧道协议

近几年出现了一些新的隧道技术, 主要工作在开放系统互连 (OSI) 参考模型中的第四和第五层^[5], 这里做一个简单的介绍, 具体包括:

4.3.1 SSL 隧道协议

SSL (Secure Socket Layer) 是 Netscape 公司设计的主要用于 web 的安全传输协议。SSL 被设计为使 TCP 提供一个可靠的端到端的安全服务, 它不是一个单一的协议, 而是由多个协议组成, 包括 SSL 记录协议 (SSL Record Protocol)、SSL 握手协议 (SSL Handshake-Protocol)、SSL 修改密文规约协议 (SSL ChangeCipher Spec Protocol)、SSL 警告协议 (SSL Alert Protocol), 其体系结构如图 3 所示。

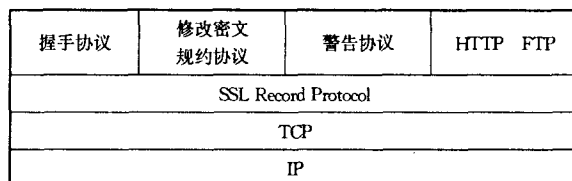


图 3 SSL 体系结构

记录协议定义了要传输数据的格式, 它位于可靠的传输协议 TCP 之上, 用于各种更高层协议的封装。记录协议主要完成分组和组合, 压缩和解压缩, 以及消息认证和加密等功能。所有传输数据包括握手消息和应用数据都被封装在记录中。握手协议允许服务器与客户机在应用程序传输和接收数据之前互相认证、协商加密算法和密钥。通信双方首先通过 SSL 握手协议建立客户端与服务器之间的安全通道, SSL 记录协议通过分段、压缩、添加 MAC 以及加密等操作步骤把应用数据封装成多条记录, 最后再进行传输。

4.3.2 SOCKS V5 隧道协议

SOCKS v5 工作在 OSI (Open System Internet) 模型中的第五层——会话层, 可作为建立高度安全的 VPN 基础。SOCKS v5 协议的优势在于访问控制, 因此适用于安全性较高的 VPN。SOCKS v5 现在被 IETF (互联网工程任务组) 建议作为建立 VPN 的标准^[6]。它的优点是能够非常详细地进行访问控制, 即在网络层只能根据源目的 IP 地址允许或拒绝被通过, 在会话层控制手段更多一些; 由于工作在会话层, 能同低层协议如 IPV4、IPSec、PPTP、L2TP 一起使用; 用 SOCKS v5 的代理服务器可隐藏网络地址结构^[7]; 能为认证、加密和密钥管理提供“插件”模块, 让用户自由地采用所需要的技术; SOCKS v5 可根据规则过滤数据流, 包括 Ja-

va Applet 和 Actives 控制。但是,它也有不少令人遗憾之处:性能比低层次协议差,必须制定更复杂的安全管理策略。这样,它最适合用于客户机到服务器的连接模式,适用于外部网 VPN 和远程访问 VPN。

5 隧道技术的实现

对于像 PPTP 和 L2TP 这样的第 2 层隧道协议,创建隧道的过程类似于在双方之间建立会话;隧道的两个端点必须同意创建隧道并协商隧道各种配置变量,如地址分配,加密或压缩等参数。绝大多数情况下,通过隧道传输的数据都使用基于数据报的协议发送。隧道维护协议被用来作为管理隧道的机制。

第 3 层隧道技术通常假定所有配置问题已经通过手工过程完成。这些协议不对隧道进行维护。与第 3 层隧道协议不同,第 2 层隧道协议(PPTP 和 L2TP)必须包括对隧道的创建、维护和终止。

隧道一旦建立,数据就可以通过隧道发送。隧道客户端和服务端使用隧道数据传输协议准备传输数据。例如,当隧道客户端向服务端发送数据时,客户端首先给负载数据加上一个隧道数据传送协议包头^[2],然后把封装的数据通过互联网络发送,并由互联网络将数据路由到隧道的服务端。隧道服务端收到数据包之后,去除隧道数据传输协议包头,然后将负载数据转发到目标网络。

因为第 2 层隧道协议(PPTP 和 L2TP)以完善的 PPP 协议为基础,因此继承了一整套的特性。

(1) 用户验证。

第 2 层隧道协议继承了 PPP 协议的用户验证方式^[1]。许多第 3 层隧道技术都假定在创建隧道之前,隧道的两个端点相互之间已经了解或已经经过验证。一个例外情况是 IPsec 协议的 ISAKMP 协商提供了隧道端点之间进行的相互验证。

(2) 令牌卡(Tokencard)支持。

通过使用扩展验证协议(EAP),第 2 层隧道协议能够支持多种验证方法,包括一次性口令(one-timepassword),加密计算器(cryptographic calculator)和智能卡等。第 3 层隧道协议也支持使用类似的方法,例如,IPsec 协议通过 ISAKMP/Oakley 协商^[6]确定公共密钥证书验证。

(3) 动态地址分配。

第 2 层隧道协议支持在网络控制协议(NCP)协商机制^[6]的基础上动态分配客户地址。第 3 层隧道协议通常假定隧道建立之前已经进行了地址分配。目前 IPsec 隧道模式下的地址分配方案仍在开发之中。

(4) 数据压缩。

第 2 层隧道协议支持基于 PPP 的数据压缩方式。例如,微软的 PPTP 和 L2TP 方案使用微软点对点加密协议(MPPE)^[7]。IETP 正在开发应用于第 3 层隧道协议的类似数据压缩机制。

(5) 数据加密。

第 2 层隧道协议支持基于 PPP 的数据加密机制。微软的 PPTP 方案支持在 RSA/RC4 算法的基础上选择使用 MPPE。第 3 层隧道协议可以使用类似方法,例如,IPsec 通过 ISAKMP/Oakley 协商确定几种可选的数据加密方法。微软的 L2TP 协议使用 IPsec 加密保障隧道客户端和服务端之间数据流的安全。

(6) 密钥管理。

作为第 2 层协议的 MPPE 依靠验证用户时生成的密钥,定期对其更新。IPsec 在 ISAKMP 交换过程中公开协商公用密钥^[5],同样对其进行定期更新。

(7) 多协议支持。

第 2 层隧道协议支持多种负载数据协议,从而使隧道客户能够访问使用 IP,IPX,或 NetBEUI 等多种协议企业网络^[7]。相反,第 3 层隧道协议,如 IPsec 隧道模式只能支持使用 IP 协议的目标网络。

6 结束语

VPN 技术已成为流行的网络技术,在社会各系统、阶层都得到了广泛应用,并能够良好运行和稳定工作。它的高度灵活性能和可靠网络安全管理措施使超大型网络建设成为可能。随着 Internet 基础设施的发展,VPN 技术必将将在校园网建设等各领域,发挥越来越重要的作用。

参考文献:

- [1] 隆益民. 远程视频会议系统的构建[J]. 网络安全技术与应用, 2006(11): 73-74.
- [2] 沈鑫刻. IP 交换网原理、技术及实现[M]. 北京: 人民邮电出版社, 2003.
- [3] 王 达. 虚拟专用网(VPN)精解[M]. 北京: 清华大学出版社, 2005.
- [4] 周 莹. 共享网络资源, 挖掘计算机潜能[J]. 微型机与应用, 1999, 18(9): 35-38.
- [5] Deal R. Cisco VPN 完全配置指南[M]. 北京: 人民邮电出版社, 2007.
- [6] 赵慧玲, 张国宏, 胡 琳, 等. ATM、帧中继、IP 技术与应用[M]. 北京: 电子工业出版社, 2000.
- [7] 李普聪. 多校区 IP 语音平台的设计与实现[J]. 计算机工程与设计, 2007, 28(9): 2220-2223.