文章编号:1006-544X(2004)03-0365-04

VPN技术及其在企业网络安全技术中的应用

李春泉[1,2], 周德俭[3], 吴兆华[1]

(1. 桂林电子工业学院 机电与交通工程系, 广西 桂林 541004; 2. 上海大学 CIMS 中心, 上海 200072;
3. 桂林工学院, 广西 桂林 541004)

摘 要: 如何构建既安全又廉价的企业网络是当前企业信息化实施的重要基础问题. 提出了基于多VPN级联的网络安全技术体系. 在分析VPN关键技术基础上, 给出了VPN的基本框架及多VPN的典型企业网络安全实现方案, 经实例验证, 很好的解决了企业网络安全与廉价兼顾的问题.

关键词: 多VPN; IPSec; 网络安全

中图分类号: TP309.2; TP393.4 **文献标识码:** A①

当前我国正在大力推行企业信息化建设, 利用计算机技术, 实现企业的设计、生产、制造、管理等一系列环节的数字化运行, 其中的关键技术就是网络技术. 如何以较低廉的成本拥有安全、可靠的网络成为摆在企业面前的一个重要问题. 基于多VPN的网络安全技术可以很好的解决企业网络安全与低成本兼顾的问题.

1 VPN的安全机理

1.1 VPN概念

VPN (Virtual Private Network, 虚拟私有网络) 是指将物理上分布在不同地点的网络通过公用网联接而成逻辑上的虚拟子网[1]. 为了保障信息在Internet上传输的安全性, VPN技术采用了认证、存取控制、机密性、数据完整性等措施, 以保证信息在传输中的安全性.

1.2 VPN的安全机理

VPN技术以隧道模式为主要的传输形式,通过在隧道头(传输双方)的加/解密操作,采用不同的隧道协议,来完成网络传输的功能. 当连接建立后, 呼叫方可以以被呼叫方子网的形式来和其他处于同一网络层次内的各网络节点进行安全的信息通信. VPN的安全主要体现在以下几个方面:

(1) 认证方法. 采用支持主要PKI厂商的PKI和一些其他兼容的X.509的PKI. 通过认证技术对用户身份进行验证, 严格控制只有授权用户才能访问VPN及拥有相应权限.

(2) 数据加/解密. 支持AES、3DES等的加密算法, 支持的密钥长度为128, 192, 256 bit等. 根据采用的加/解密算法对通过公共互联网络传递的数据进行加密, 确保网络其他未授权的用户无法读取该信息.

(3) 密钥管理. VPN技术能够生成并更新客户端和服务器的加密密钥以及密钥的分发.

(4) 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, 包括IP、IPX等.

1.3 关键技术

(1) 隧道技术[2]. 指在传输的两点之间建立起一条类似于专用“通道”的通信通道. 通过隧道将具有各种协议的数据帧或数据包重新封装新的包头后进行传输. 其连接结构如图1所示.

(2) 主要隧道协议

· 点对点隧道协议 (PPTP)

PPTP是“点对点协议 (PPP)”的扩展, 增强

① **收稿日期:** 2004-02-19

基金项目: 广西科学与技术开发项目 (0141041) 资助

作者简介: 李春泉(1975-),男,博士研究生,讲师,研究方向:SMT制造系统自动化技术,网络化制造技术,敏捷制造技术.

了 PPP 的身份验证、数据压缩和加密机制. 其允许对 IP、IPX 或 NETBEUI 数据流加密，然后经封装后通过互联网络发送. 封装使用一般路由封装（GRE）头文件和 IP 头数据包装 PPP 帧（一个 IP 数据包、一个 IPX 数据包或一个 NetBEUI 帧）. 加密使用由 MS－CHAP 或 EAP－TLS 身份验证过程中生成的密匙，其客户机必须使用 MS－CHAP 或 EAP－TLS 身份验证协议. 图 2 所示为 PPP 帧的 PPTP 封装.

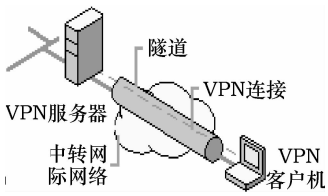

图 1 隧道技术

Fig. 1 Tunneling protocol

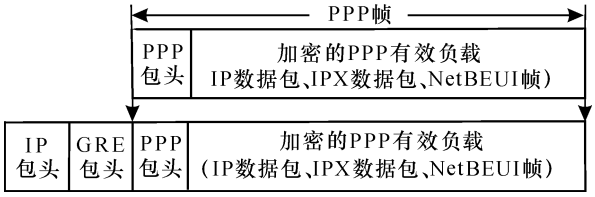

图 2 点对点隧道协议（PPTP）

Fig. 2 PPTP tunneling protocol

·安全 IP（IPSec）隧道模式

IPSec（IP Security）用于提供 IP 层的安全性. 允许对 IP 负载数据进行加密，然后封装在 IP 包头中通过企业 IP 网络或公共 IP 互联网络如 Internet 发送（图 3）. 在 IPSec 中有 3 个主要协议：AH，ESP 和 IKE. ESP（Encapsulating Security Payload）协议主要用来处理对 IP 数据包的加密. 几乎可以支持各种对称密钥加密算法. AH（Authentication Header）除了可以对 IP 的负载进行认证外，还可以对 IP 头部实施认证. 主要是处理数据对，可以对 IP 头部进行认证. IKE（Internet Key Exchange）协议主要是对密钥交换进行管理，包括密钥协商、密钥交换机制和约定跟踪 3 个功能.

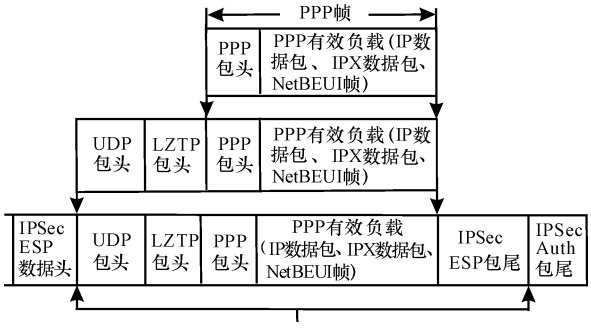

图 3 安全 IP（IPSec）隧道模式

Fig. 3 IPSec tunneling protocol

2 企业信息化网络安全技术

2.1 VPN 技术的基本框架

VPN 的实现包含管理模块、密钥分配和生成模块、身份认证模块、数据加密/解密模块、数据传送模块几部分[3]（图 4）.

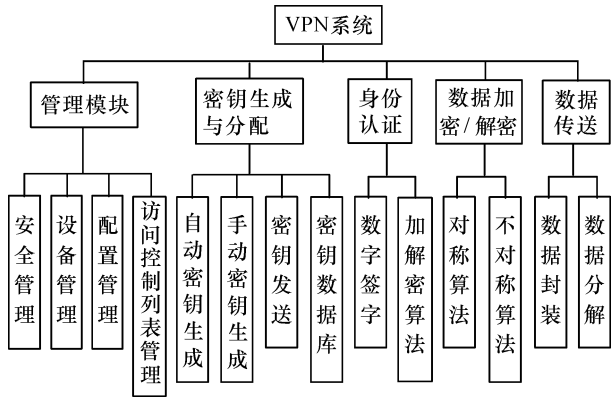

图 4 VPN 技术的基本框架

Fig. 4 Basic framework of VPN

管理模块负责整个系统的管理. 可以决定传输模式，密钥生成、分配方式，数据包加密/解密模式等.

密钥管理模块负责完成身份认证和数据加密所需的密钥生成和分配. 密钥的生成采取自动/手动随机生成的方式，密钥的分配采用手动、非网络传输分配的方式.

身份认证模块对 IP 数据包完成数字签名的运算与认证. 数字签名在保证数据完整性的同时，也起到了身份认证的作用.

数据加密/解密模块完成对 IP 数据包的加密和解密操作. 加密算法有对称加密算法和非对称加密算法（如 DES 算法和 IDEA 算法）. 也可以采用专用硬件的方式实现数据的加密和解密.

数据传送的实现包含数据分组的封装模块和封装分解模块两部分. 当从安全网关发送 IP 数据分组时，数据分组封装/分解模块为 IP 数据分组附加上身份认证头 AH 和安全数据封装头 ESP. 接收方收到数据分组时，数据分组封装/分解模块对

AH 和 ESP 进行协议分析，并根据包头信息进行身份验证和数据解密.

2.2　多 VPN 的典型企业网络安全实现方案

多 VPN 的典型企业网络安全实现方案（图 5）构建了企业多级级联的 VPN 网络安全结构[4].

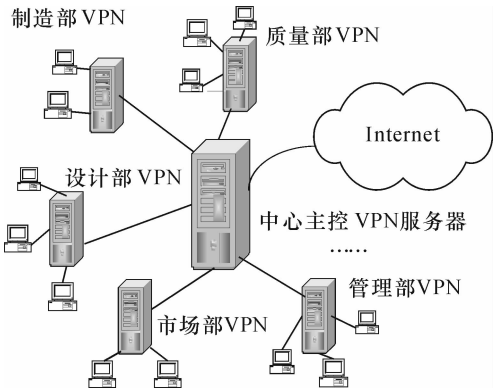

图 5　多 VPN 的典型企业网络安全实现方案
Fig. 5　Scheme of enterprise network security multi-VPN

通过设定访问的密钥与权限，外界访问者（企业协作者）通过中心 VPN 被指定安全级别与种类，与特定的部门进行连接；同时，各子系统 VPN 一方面将中心 VPN 通过的信息传递至本系统内部，另一方面，子系统的信息经部门 VPN 信息安全加密后，传送至中心 VPN，再经由中心 VPN 的安全检查与数据加密后，与外界沟通. 而各部门之间也经由中心 VPN 的安全机制进行数据的交流与协作. 通过这样的网络安全结构，充分保证了数据的安全与便捷，同时，企业间的协作可以在部门之间实现.

3　实例验证

图 6 所示为 VPN 的一个实例. 客户端的计算机可以通过 Internet 与 VPN 服务器相连，在经过 VPN 的认证、存取控制、机密性、数据完整性等措施后，与企业内部私网处于同一个逻辑网络层次内，进而达到与局域网内部的数据交流与数据安全.

3.1　VPN 软件环境

服务器端：

Windows 2000 Server，Service Pack 3，Routing and Remote Access Service

客户端：Windows 98

3.2　网络环境

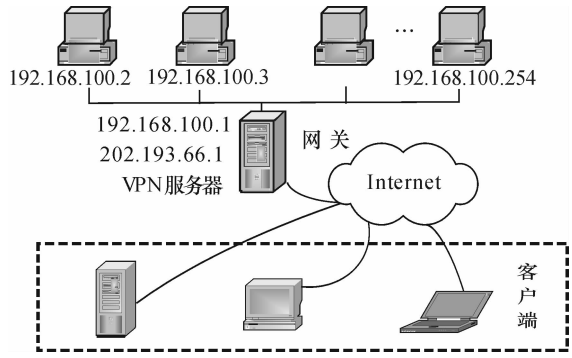

图 6　VPN 应用实例
Fig. 6　Instance of VPN application

（1）VPN 服务器. VPN 服务器包含了 2 个 IP 地址：202. 193. 66. 1 作为企业公网 IP 地址，192. 168. 100. 1 作为企业内网 IP 地址.

（2）企业内部网络. 内部局域网私有网络地址为：192. 168. 100. 2/254，子网掩码：255. 255. 255. 0.

（3）客户端网络. 客户端网络是与 VPN 的企业公网 IP 处于不同物理网段的外部网络.

3.3　安装 VPN

在 VPN 服务器上安装 VPN.

（1）选择隧道协议. 根据安全性要求与需要，选择 PPTP、L2TP 和 Ipsec. 本文选择了最简单的 PPTP 隧道协议，其它协议类似.

（2）安装 Windows 2000 服务. 选择安装 Routing and Remote Access Service（Routing & RAS）服务.

（3）设置 Routing & RAS 属性. ①设置连接 VPN 通道数目；②设置 VPN 网络存取范围、允许协议、授权方案、IP 动/静态分配等.

（4）添加 VPN 访问用户. 根据访问的需要，添加远程拨入 VPN 帐号.

3.4　创建 VPN 客户端 VPN 访问软件包

利用 Windows 2000 Server 中的“连接管理器管理工具”，创建 VPN 客户端 VPN 访问软件包. 将此软件包分发至客户端，客户端就可以利用此软件包进行 VPN 访问连接.

3.5　测试 VPN 连接

（1）建立前. 在服务器端未建立（或启动）VPN 连接时，可利用 Ping（或 Tracert）操作，进行两个测试：企业内部网络访问外部客户端；外部客户端访问企业内部网络. 由于未建立 VPN 连

接，两个 Ping 结果均如下：Request timed out.

（2）建立后. 在服务器端建立（或启动）VPN 连接时，同样可以利用 Ping（或 Tracert）操作，进行两个测试：

· 内部到外部. 设外部客户端 IP 为 202. 193. 58. 220，ping 结果如下：

Reply from 202. 193. 58. 220：bytes = 32 time < 10 ms TTL = 128

· 外部到内部. 用 Ping 访问 VPN 服务器，结果如下：

Reply from 192. 168. 100. 1：bytes = 32 time = 10 ms TTL = 128

用 Ping 访问 VPN 内部局域网，结果如下：

Reply from 192. 168. 100. 2：bytes = 32 time = 10 ms TTL = 128

由于 VPN 连接是将外部客户端的连接进行企业内部网 IP 动/静态分配，从而使外部客户端与企业内部网络处于同一逻辑网段内，所以，可以用 Ipconfig 来获得外部客户端在企业内部网的 IP 地址，得到如下结果.

Ethernet adapter 本地连接：

IP Address：202. 193. 58. 220

Subnet Mask：255. 255. 255. 0

Default Gateway：202. 193. 58. 254

PPP adapter 虚拟专用连接：

IP Address：192. 168. 100. 5

Subnet Mask：255. 255. 255. 0

Default Gateway：192. 168. 100. 1

其中 IP：202. 193. 58. 220 为客户端公网 IP 地址，IP：192. 168. 100. 5 为客户端在企业私网中分配的 IP 地址.

本文是以简单 VPN 连接为例，多 VPN 级联的建立与验证过程相似.

4 结 论

VPN 技术是近年新兴起的一项网络安全技术，在体系上，它隶属于 Ipv6，是未来互联网发展的一个重要方向. 本文提出了基于多 VPN 级联的网络安全技术体系. 在分析了 VPN 的关键技术基础上，提出了 VPN 的基本框架及多 VPN 的典型企业网络安全实现方案，很好的解决了企业网络安全与低成本兼顾的问题. 最后，通过实例进行了 VPN 的实现与测试.

参考文献

[1] 许 勇，张 凌，郝志锋，等. 基于 VPN 的企业内联网[J]. 计算机工程与应用，2001，(23)：33 - 34.

[2] 汪海航，谭成翔，孙为清，等. VPN 技术的研究与应用现状及发展趋势[J]. 计算机工程与应用，2001，(23)：14 - 16.

[3] 屈长青，魏大宽. 基于 IPSec 的 VPN 技术[J]. 计算技术与自动化，2001，20 (4)：63 - 66.

[4] Shorrock G，Awdry C. Concert IP secure—a managed firewall and VPN service [J]. BT Technol，2001，19 (3)：99 - 106.

VPN and its application in enterprise network security technology

LI Chun-quan[1,2]，ZHOU De-jian[3]，WU Zhao-hua[1]

(1. *Department of Electronic Machinery and Traffic Engineering*，*Guilin University of Electronic Technology*，*Guilin* 541004，*China*；2. *CIMS Center*，*Shanghai University*，*Shanghai* 200072，*China*；3. *Guilin Institute of Technology*，*Guilin* 541004，*China*)

Abstract：The method of constructing secure and low-cost enterprise network is important for enterprises. It's also a basic issue for enterprises information. The system of network security technology based on multi-VPN is discussed. The key technology of VPN is studied. Basic framework of VPN & scheme of enterprise network security based on multi-VPN concerning both security and low cost are put forward and proved to be applicable in the testing.

Key words：multi-VPN；IPSec；network security