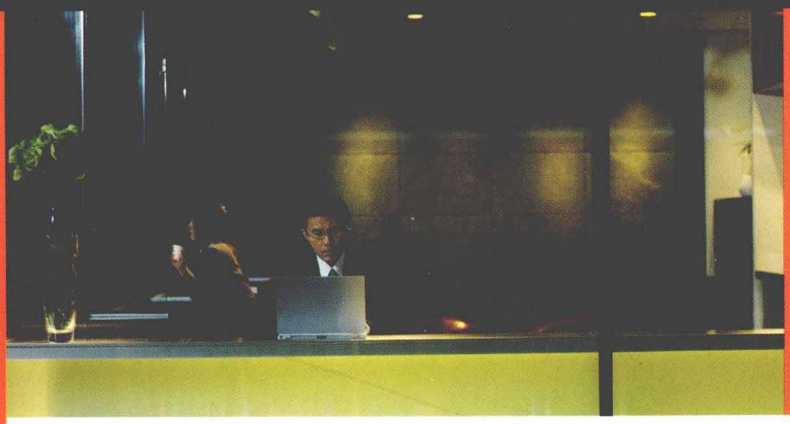
CISCO

ciscopress.com



SECURITY

IPSec VPN设计

IPSec VPN Design

The definitive design and deployment guide for secure virtual private networks

Vijay Bollapragada, CCIE #1606
〔美〕 **Mohamed Khalid,** CCIE #2435 著
Scott Wainner
袁国忠 译

人民邮电出版社
POSTS & TELECOM PRESS

ciscopress.com

IPSec VPN设计

IPSec VPN Design

Vijay Bollapragada, CCIE #1606
〔美〕 **Mohamed Khalid,** CCIE #2435 著
Scott Wainner
袁国忠 译

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

IPSec VPN设计 / (美) 波拉普拉哥达(Bollapragada,V.)，(美) 哈利德 (Khalid,M.)，(美) 维纳 (Wainner,S.) 著；袁国忠译. -- 北京：人民邮电出版社，2012.11
ISBN 978-7-115-29577-4

Ⅰ. ①I… Ⅱ. ①波… ②哈… ③维… ④袁… Ⅲ. ①互联网络－传输控制协议 Ⅳ. ①TP393.4

中国版本图书馆CIP数据核字(2012)第231977号

版 权 声 明

IPSec VPN 设计

◆ 著 [美] Vijay Bollapragada, CCIE #1606
Mohamed Khalid, CCIE #2435
Scott Wainner
译 袁国忠
责任编辑 傅道坤

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子邮件 315@ptpress com cn
网址 http //www ptpress com cn
北京艺辉印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：19 5
字数：410 千字 2012 年 11 月第 1 版
印数：1－3 000 册 2012 年 11 月北京第 1 次印刷

著作权合同登记号 图字：01-2012-4891 号
ISBN 978-7-115-29577-4

定价：55 00 元

读者服务热线：(010)67132692 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

IPSec 是一种流行的 VPN 技术，有关 IPSec 协议的技术细节和产品级配置的图书很多，但都没有讨论 IPSec VPN 总体设计方面的问题，本书旨在填补这一空白，帮助读者在各种环境中部署高效、安全的 IPSec VPN 解决方案。

本书详细讨论了 IPSec VPN 设计，引导读者深入理解大型 IPSec VPN 解决方案的设计和架构。本书共分为三部分，第一部分全面介绍了 IPSec 架构，包括 IPSec 协议及 Cisco IOS IPSec 实现细节；第二部分讨论了 IPSec VPN 设计原则，包括星型（hub-and-spoke）和全互联拓扑及容错设计，还介绍了用于简化 IPSec VPN 配置的动态配置模型；第三部分讨论了在 IPSec VPN 中支持语音和多播等应用涉及的问题，探讨了如何高效地集成 IPSec VPN 和 MPLS VPN。

本书适合从事 IPSec VPN 设计、部署和故障排除的网络从业人员阅读，也适合备考 Cisco 相关认证的考生阅读。

关于作者

Vijay Bollapragada，CCIE #1606，是 Cisco 公司网络系统集成与测试工程组的主管，致力于复杂网络解决方案的架构、设计和验证工作。作为一名路由器体系结构和 IP 路由领域的专家，Vijay 与他人合著了 *Inside Cisco IOS Architecture* 一书（由 Cisco Press 出版），他还是杜克大学电子工程系的副教授。

Mohamed Khalid，CCIE #2435，是 Cisco 公司负责 IP VPN 解决方案的一位技术领导。他与全球的服务提供商以及与其相关的 Cisco 客服团队展开广泛合作，以针对不同的 IP VPN 体系结构确定其技术和工程需求。

Scott Wainner 是 Cisco 公司美国服务提供商销售部门的一位杰出的系统工程师，致力于 VPN 体系结构和解决方案的开发。凭借他在这方面的专长，他以咨询人员的身份直接与客户打交道，在解释客户需求并推动 Cisco 公司内部开发举措的同时，还为客户提供 IP VPN 体系结构方面的指导。在网络行业，Scott 具有 18 年之久的从业经验，从事过众多的工作，其中包括网络运维、网络安装/供应、网络工程和产品工程。最近，他主要致力于 L2VPN 和 L3VPN 服务模型的研究，这些服务模型使用 MPLS VPN、虚拟线路模拟和 IPSec/SSL 为企业和服务提供商提供 VPN 服务。他拥有美国空军学院电子工程专业的学士学位，以及乔治梅森大学（位于弗吉尼亚的费尔法克斯市）电子和计算机工程专业的硕士学位。Scott 当前是 IEEE 和 IETF 的活跃成员。

关于技术编辑

Anthony Kwan 是 HTA 的董事兼基础设施项目的执行经理，持有 CCNP、CCDP、MCSE、Master ASE、MCNE 和 CCIE（笔试）证书。他在网络互联行业有 10 年的从业经验，设计并组建了大量安全的企业数据中心，其中一个数据中心的预算高达 1.2 亿美元。他还就网络基础设施和技术咨询场地的建设方面，为多家咨询公司提供指导。他还经常为 Cisco Press 和其他网络技术专业的出版物撰稿。

Suresh Subbarao 在近 10 年一直从业于网络行业，他当前是 Cisco 公司的一名网络工程师，致力于为服务提供商提供安全服务，其关注重点是 IPSec VPN。

Michael Sullenberger 于 1981 年从哈维玛德学院获数学学士学位，并于当年成为斯坦福直线加速器中心（Stanford Linear Accelerator Center，SLAC）的一名 Fortran 程序员和 BITnet 网络（速度为 9600 波特的早期 WWW 网络）的用户，从而进入计算机网络领域。在 SLAC 期间，Michael 还负责管理 DEC VMS 计算机，从而熟悉了 DECnet 和 LAT 协议。他还参与了将以太网和 FDDI 网络引入 SLAC 的工作。1988 年，Michael 进入网络小组，协助将一个大型桥接（主要是 DECnet）网络转换为一个路由式多协议（主要是 TCP/IP）网络。1994 年，他离开 SLAC，跳槽到小型公司 TGV，该公司致力于为 OpenVMS 和 Windows 系统开发 TCP/IP 协议栈和应用程序。在 TGV 期间，他从事技术支持工作，熟悉了从 IP 层到应用层的 TCP/IP 细节。1996 年，TGV 被 Cisco 收购，Michael 加入到路由选择协议组，熟悉了链路层和 IP 路由选择协议，TCP/IP 的知识得以进一步提高。1998 年，Michael 进入 Cisco 升级小组（Escalation Team），从而熟悉

了 NAT、HSRP、GRE 和 IPSec 加密等领域，其 TCP/IP 知识再一次得以提高。2000 年，他担任一个项目的首席架构师，该项目成了用于扩展 IPSec VPN 网络的 Cisco 动态多点 VPN（DMVPN）解决方案。2004 年，DMVPN 解决方案获得了 Cisco 先锋奖。到目前为止，Michael 一直从事 DMVPN 的改进以及 DMVPN 和 IPSec 网络的设计和故障排除工作。另外，从 2000 年起，Michael 开始每年都在 Cisco Networkers 会议上发表有关站点到站点 IPSec 到 DMVPN 网络的演讲。

献　　词

Vijay Bollapragada：献给我最好的朋友也是我的妻子 Leena，谢谢她的关爱和鼓励，谢谢她允许我将宝贵的家庭时间用来写作本书。献给我的父母，谢谢他们给我灌输了正确的价值观。献给我的两位爱子 Amita 和 Abhishek 以及周围的好友。

谢谢我的合著者 Mo 和 Scott，我在编写本书期间历经考验和磨难，是他们给予了包容，并鼓励我坚持下去。谢谢 Cisco 的那一票好友，他们不断让我接受挑战，并不时提醒我“每天都有新的东西要学习”。

Mohamed Khalid：首先我要感谢我的父母，是他们的奉献、牺牲和鼓励，促使我走向成功，取得今天的成就。谢谢我的妻子 Farhath，她给了我时间和持续的勇气，我才得以完成本书的写作。

谢谢 Scott Wainner、Haseeb 和 Sunil 在技术方面提供了宝贵的意见。最后，我还要郑重感谢我的朋友兼本书的合著者 Vijay Bollapragada，是他“引诱”我合著本书，并在本书的编写过程中给予我鼓励和帮助，直至本书完成。

Scott Wainner：我要感谢我的妻子 Jill，谢谢她给予的关爱、容忍和鼓励。由于我每天的时间有限，是她托付起了整个家庭的重任。我还要谢谢我的孩子 Craig、Brett、Natalie 和 Caroline，谢谢他们在探索人生期间表现出来的耐心和灵感。

还要特别感谢我的父母 Tom 和 Zenith，他们在我的生活中给予了启发和引导。谢谢我的同事 Vijay 和 Mo，这几年能和你们一起共事是我的荣幸。最后，还要感谢我的神，谢谢他让我实现这个写书的梦想。

致　谢

要不是有众多人为本书提供了宝贵的建议，从而提升了本书的品质，本书的出版几无可能。首先，我们要感谢本书的技术审稿人，其中也包括 Anthony Kwan、Mike Sullenberger 和 Suresh Subbarao。他们对书中的主题了如指掌，而且对细节问题也格外关注，因此提出的建议才无比真贵。我们还要感谢 Cisco Press 的 Brett Bartow，他不时给我们“施压”，并最终让本书得以面市。如果没有他的帮助，本书则没有见光之日。我们还要感谢 Cisco Press 的 Grant Munroe 和 Chirs Cleveland，他们精于细节的态度让本书的质量得以大幅提升。我们还要感谢 Cisco 公司的 IPSec 开发团队，正是因为他们编写的代码如此完美，才让本书中讨论的所有特性得以展现。

前　言

对企业和服务提供商来说，VPN 变得越来越重要。IPSec 还是一种用来部署基于 IP 的 VPN 的常见技术。市面上有关 IP Sec 协议的技术细节和产品级配置的图书很多，但都没有讨论部署 IPSec VPN 的总体设计方面的问题。

本书的目标

本书旨在帮助读者深入理解 IPSec VPN 的设计和体系结构，并在启用增值服务以及将 IPSec VPN 与其他三层（MPLS VPN）技术相集成方面为读者提供指导。

针对的读者

本书主要针对的读者是参与 IPSec VPN 设计、部署和故障排除的网络工程师。在学习本书时，尽管读者不一定非要具备 IPSec 知识，但应该对基本的 IP 路由有深入的理解。

本书的组织结构

本书分三部分。第一部分介绍 IPSec 的总体结构，其中包括 IPSec 协议及 Cisco IOS IPSec 实现细节。第二部分从第 5 章开始，讨论 IPSec VPN 设计原理，其中包括星型拓扑（hub-and-spoke）、全互联（full-mesh）和容错设计；还介绍了用于简化 IPSec VPN 设计的动态配置模型，并提供了一个案例研究。第三部分从第 8 章开始，介绍在 IPSec VPN 中提供诸如语音、多播等服务时，以及将 IPSec VPN 和 MPLS VPN 相集成时涉及的问题。本书的组织结构如下。

- **第一部分“简介和概念”**

第 1 章，“VPN 简介”，对 VPN 的概念和各种 VPN 技术进行简单的介绍。

第 2 章，“IPSec 概述”，概述 IPSec 协议，并讲解了传输模式和隧道模式之间的差异；还解释了 Cisco IOS IPSec 的分组处理过程。

第 3 章，“增强的 IPSec 特性”，简单介绍了可改进 IPSec VPN 可扩展性和容错性的 IPSec 高级特性，如失效对等体检测和控制平面的存活

机制。本章还介绍了在 IPSec VPN 中使用网络地址转换（NAT）和路径最大传输单元检测（PMTUD）面临的困难以及如何克服它们。

第 4 章，“IPSes 认证和授权模型”，讲解了主要被远程接入用户所使用的 IPSec 特性，如扩展认证（XAUTH）和模式配置（MODE-CFG），还介绍了 Cisco EzVPN 连接模型和数字证书概念。

- **第二部分“设计和部署”**

第 5 章，“IPSec VPN 架构”，介绍各种 IPSec 连接模型，如本征 IPSec、GRE 和远程接入，并探讨了每种连接模型的部署架构及其优缺点。

第 6 章，“设计容错的 IPSec VPN”，讨论如何在 VPN 架构中引入容错功能，描述使用各种容错方法时的注意事项。

第 7 章，“站点到站点 IPSec VPN 的自动配置架构”，介绍用来简化大型 IPSes VPN 配置复杂性的机制，并深入讨论隧道端点发现（TED）和动态多点 VPN（DMVPN）这两种机制。

- **第三部分“服务改善”**

第 8 章，“IPSec 和应用的互操作性”，讨论了在 IPSec VPN 中运行语音和多播等应用时将面临的问题。

第 9 章，“基于网络的 IPSec VPN”，简要地介绍了基于网络的 VPN 的概念。

本书使用的图标

命令语法约定

本书命令语法遵循的惯例与 IOS 命令手册使用的惯例相同。命令手册对这些惯例的描述如下。

- **粗体字**表示照原样输入的命令和关键字，在实际的设置和输出（非常规命令语法）中，粗体字表示命令由用户手动输入（如 **show** 命令）。
- *斜体字*表示用户应提供的具体值参数。
- 竖线（|）用于分隔可选的、互斥的选项。
- 方括号（[]）表示任选项。
- 花括号（{}）表示必选项。
- 方括号中的花括号（[{}]）表示必须在任选项中选择一个。

目　录

第 1 章

VPN 简介

虚拟专网常被称为 VPN，并非网络技术中的新概念。顾名思义，VPN 是通过公共网络基础设施提供的一种专用网络服务。最简单的虚拟专用连接是两人打电话，这是通过公共电话网络进行的。

VPN 种类众多，如帧中继和 ATM。每种 VPN 技术都可以写成一本书，也确实有这样的图书。本书介绍一种名为 IPSec 的 VPN 技术。

1.1 部署 VPN 的动机

本章简要地介绍一些 VPN 技术以及部署 VPN 的动机。部署 VPN 主要是为了减少费用。办事处遍布世界各地的公司，为开展业务经常需要将这些办事处互联起来。为建立这些连接，可以在办事处之间使用租用线；也可以让每个办事处连接到本地公共网络（如 Internet），并通过公共网络建立 VPN。

在图 1.1 中，一家跨国公司使用租用线将站点彼此相连。每条连接都是点到点的，连接到每个站点都需要一条租用线。如果每个站点都需要同其他所有站点相连（这被称为全互联），则每个站点需要 $n-1$ 条租用线，其中 n 为总站点数。租用线通常按距离和带宽收费，因此跨越整个国家和跨国的链路通常极其昂贵，这使得使用租用线实现全互联的费用非常高。

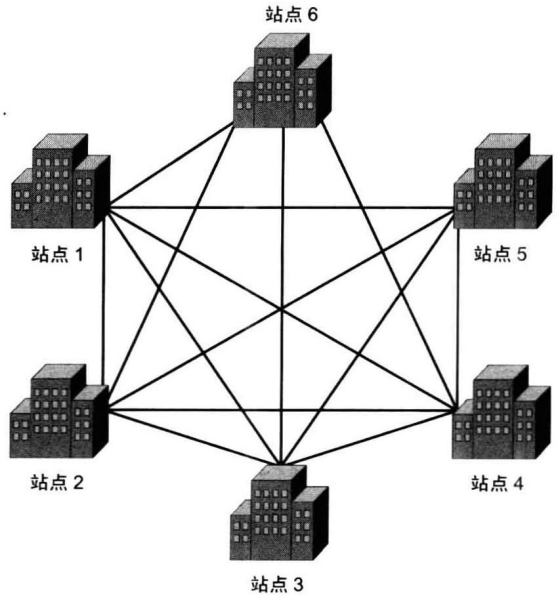


图 1.1 使用租用线将公司的站点彼此相连

在图 1.2 中，使用另一种方法来连接公司的站点：通过公共网络（如 Internet）进行连接。在这个模型中，每个站点都就近连接到公共网络（可能通过租用线），但站点之间的连接都是虚连接。图中的网络云表示站点之间的虚连接，而在租用线模型中，站点之间是物理专用连接。

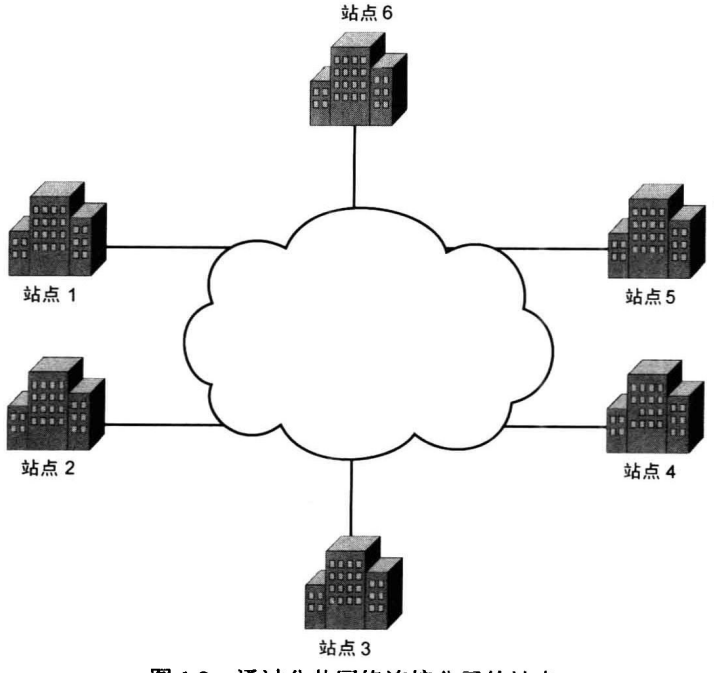


图 1.2 通过公共网络连接公司的站点

注意：公共网络是其基础设施被众多用户共享的网络。请切记，“公共”并不表示网络可供任何人免费使用。很多服务提供商都有大型的 ATM 和帧中继公共网络，而 Internet 是覆盖范围最大的公共网络。

相对于租用线模型，通过公共网络连接站点在费用方面有明显的优势，可为公司节省大笔费用，但这也带来了风险，如：

- 数据不安全；
- 站点之间没有专用带宽。

在 VPN 模型中，公司的数据必须通过公共网络进行传输，这意味着其他公共网络用户可能访问这些数据，从而带来安全风险。

VPN 模型的第二种风险是，不像租用线模型中那样站点之间有专用带宽。在 VPN 模型中，使用虚连接来连接站点，而实际使用的是公共网络中的物理链路，这些链路由很多 VPN 的众多站点共享。除非 VPN 支持某种连接许可控制和带宽预留机制，否则无法保证站点之间的带宽。这两种风险都是可以消除的，下一节将介绍一些消除这些风险的 VPN 技术。

1.2　VPN 技术

简单地说，VPN 通过公共网络连接两个端点，在它们之间建立一条逻辑连接。逻辑连接可以在 OSI 模型的第 2 层或第 3 层建立，根据逻辑连接模型，将 VPN 技术粗略地划分为第 2 层 VPN 和第 3 层 VPN。从概念上说，通过第 2 层 VPN 和第 3 层 VPN 在站点之间建立的连接性是相同的。需要在有效负载的前面加上“递送报头”，以便将其传输到目标站点。在第 2 层 VPN 中，递送报头位于第 2 层；而在第 3 层 VPN 中，递送报头位于第 3 层。ATM 和帧中继都是第 2 层 VPN；而 GRE、L2TP、MPLS 和 IPSec 属于第 3 层 VPN 技术。

1.2.1　第 2 层 VPN

第 2 层 VPN 运行在 OSI 参考模型的第 2 层，它们是点到点的，通过虚电路在站点之间建立连接性。虚电路是网络中两个端点之间的逻辑端到端连接，可以跨越网络中的多个网络元件和物理网段。虚电路被配置成端到端的，通常被称为永久虚电路（PVC）。虚电路也可以是动态点到点的，这被称为交换虚电路（SVC）；由于其故障排除很复杂，因此不那么常用。ATM 和帧中继是两种最流行的第 2 层 VPN 技术，它们能够为公司提供站点到站点的连