Cisco Systems

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

IPSec VPN设计

Vijay Bollapragada, CCIE #1606
[美] Mohamed Khalid, CCIE #2435 著
Scott Wainner

袁国忠 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

IPSec VPN 设计 /（美）博兰普拉格德（Bollapragad a，V.），（美）肯哈利德（Khalid，M.），（美）韦恩纳（Wainner，S.）著；袁国忠译．—北京：人民邮电出版社，2006.5
ISBN 7-115-14626-8

Ⅰ．I…　Ⅱ．①博…②肯…③韦…④袁…　Ⅲ．因特网—传输控制协议　Ⅳ．TP393.4

中国版本图书馆 CIP 数据核字（2006）第 023381 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　李　际

◆ 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　电子函件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

◆ 开本：787×1092　1/16

印张：17.75

字数：431 千字　2006 年 5 月第 1 版

印数：1－3 500 册　2006 年 5 月北京第 1 次印刷

著作权合同登记号　图字：01-2006-0303 号

ISBN 7-115-14626-8/TP・5313

定价：39.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223

内容提要

IPSec是流行的VPN技术之一，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，是有关这方面内容的开山之作。全书包括三部分，引导读者深入理解大型IPSec VPN解决方案的设计和架构。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设计问题，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工程师阅读。

作者简介

Vijay Bollapragada（CCIE No. 1606）是Cisco Systems公司网络系统集成和测试工程小组的主管，从事复杂网络解决方案的架构设计和验证工作。他是路由器架构和IP路由选择方面的专家，同他人合著了Cisco Press出版的图书*Inside Cisco IOS Software Architecture*。他也是杜克大学电子工程系的副教授。

Mohamed Khalid（CCIE No. 2435）是Cisco Systems公司IP VPN解决方案方面的技术带头人。同大量服务提供商及其Cisco Account小组合作，确定各种IP VPN架构的技术和工程需求。

Scott Wainner是Cisco Systems公司美国服务提供商销售组织的一名杰出系统工程师，主要从事VPN架构和解决方案的开发工作。在这个职位上，他以咨询人员的身份直接同客户打交道，提供有关IP VPN架构的指导；同时，解释客户的需求，推动Cisco Systems内部的开发。Scott有18年的网络行业从业经验，从事过众多的工作，其中包括网络运营、网络安装/供应、管理和产品设计。最近，他的主攻方向为使用MPLS VPN、伪线路模拟和IPSec/SSL，为企业和服务提供商提供VPN服务的L2VPN和L3VPN服务。他拥有美国空军学院的电子工程学士学位和George Mason大学的电子和计算机工程硕士学位。Scott当前是活跃的IEEE和IETF成员。

技术编辑简介

Anthony Kwan是HTA的董事兼基础设施项目执行经理，获得CCNP、CCDP、MCSE、Master ASE、MCNE和CCIE证书，拥有10年的互连网络行业从业经验，设计并组建了大量的安全企业数据中心，其中最高预算达12亿美元。他还指导过众多咨询公司从事网络基础设施的构建和技术咨询工作，经常为Cisco Press和其他网络技术出版物撰稿，其电子邮箱为atonio888@yahoo.com。

Suresh Subbarao近10年来一直从业于网络行业，现为Cisco Systems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，重点是IPSec VPN。

Michael Sullenberger于1981年从Harvey Mudd College获数学学士学位，并于当年成为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DECVMS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进入网络技术小组，协助将一个大型桥接（主要是DECnet）网络转换为一个路由型多协议（主要是TCP/IP）网络。1994年，他离开SLAC，跳槽到小型公司TGV，该公司致力于开发TCP/IP协议栈以及OpenVMS和Windows系统应用程序。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小组，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，TCP/IP知识再一次得以进一步提高。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 Pioneer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一直在每年一次的思科用户大会（Networkers Conferences）上发表有关场点到场点IPsec和DMVPN网络的演讲。

前　言

对企业和服务提供商来说，VPN变得越来越重要。IPSec是目前流行的基于IP的VPN部署技术之一。市面上有关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的设计和架构，指导读者提供增值服务以及集成IPSec VPN和其他第3层（MPLS VPN）技术。

针对的读者

本书针对的主要读者是参与IPSec VPN设计、部署和故障排除的网络工程师；假定读者对基本的IP路由选择有深入了解，但不要求掌握了IPSec知识。

本书的组织结构

本书分三部分。第一部分介绍IPSec通用架构，包括其协议及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，包括星型拓扑（hub-and-spoke）、全互联（full-mesh）和容错设计；还将介绍用于简化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、多播等服务时涉及的设计问题以及如何集成IPSec VPN和MPLS VPN。本书的组织结构如下：

• 第一部分“简介和概念”

第1章“VPN简介”：概述VPN概念和各种VPN技术。

第2章“IPSec概述”：概述IPSec协议，介绍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”：简要地介绍可改善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“IPSec认证和授权模型”：探讨为支持远程接入用户所需的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；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架构中加入容错功能，描述使用各种容错方法时的注意事项。

第7章“场点到场点IPSec VPN的自动配置架构”：介绍简化大型IPSec VPN配置的机制，深入讨论的两种机制是隧道端点发现（TED）和动态多点VPN（DMVPN）。

• 第三部分“服务改善”

第8章“IPSec和应用互操作性”：讨论了在IPSec VPN中运行诸如语音和多播等应用将面临的问题。

第9章“基于网络的IPSec VPN”：简要地介绍了基于网络的VPN。

本书使用的图标

命令语法约定

本书在介绍命令语法时使用的约定与《IOS命令参考手册》相同，这些约定如下：

• 需要逐字输入的命令和关键字用**粗体**表示。在配置范例和输出（而不是命令语法）中，需要用户手工输入的命令用**粗体**表示（如命令**show**）。

• 用户必须提供实际值的参数用*斜体*表示。

• 互斥的元素用竖线（|）隔开。

• 可选元素用方括号（[ ]）括起。

• 必不可少的选项用大括号（{ }）括起。

• 可选元素中必不可少的选项用[{ }]括起。

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技术都可以写一整本书，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连起来。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场点彼此相连。

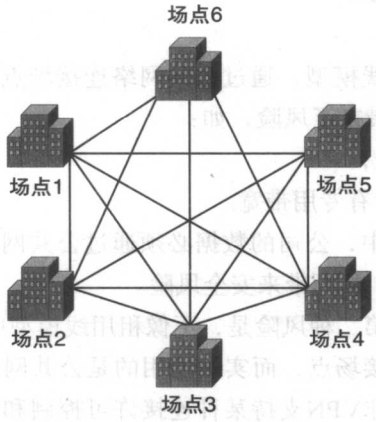

图1.1 使用租用线将公司的场点彼此相连

每条连接都是点到点的，连接到每个场点都需要一条租用线。如果每个场点都需要同其他所有场点相连（这被称为全互联），则每个场点需要n-1条租用线，其中n为总场点数。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。

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

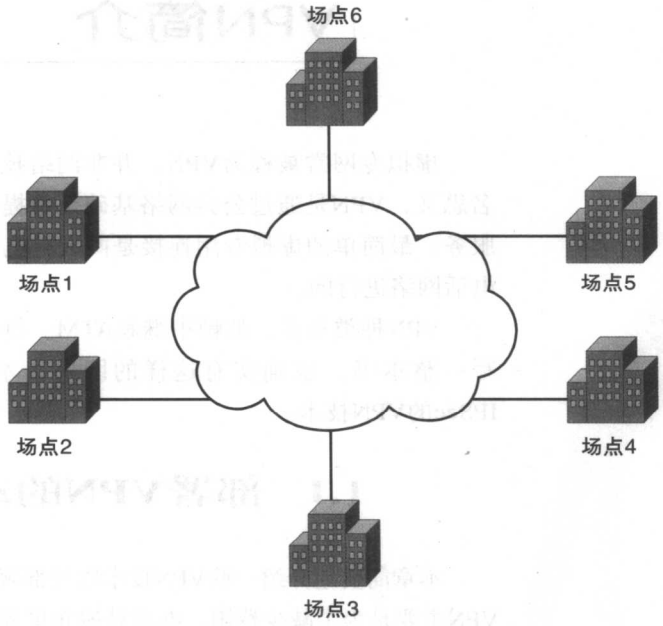

图1.2 通过公共网络连接公司的场点

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，通过公共网络连接场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；
- 场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场点之间有专用带宽。在VPN模型中，使用虚连接来连接场点，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的众多场点共享。除非VPN支持某种连接许可控制和带宽预留机制，否则无法保证场点之间的带宽。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在场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场点。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，通过虚电路在场点之间建立连接性。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场点到场点的连接性，这是通过配置跨越公用主干的永久虚电路实现的。

第2层VPN的优点之一是，独立于它传输的第3层数据流有效负载。场点之间的帧中继或ATM PVC能够传输多种不同的第3层数据流，如IP、IPX、AppleTalk、IP多播等。ATM和帧中继还具有良好的服务质量（QoS）特征，这对于诸如语音等对延迟敏感的数据流至关重要。

1.2.2 第3层VPN

如果递送报头位于OSI模型的第3层，则场点之间的连接为第3层VPN。常见的第3层VPN包括GRE、MPLS和IPSec VPN。第3层VPN可以以点到点的方式连接两个场点，如GRE和IPSec，也可以在众多场点之间建立全互连连接性，如MPLS VPN。

1. GRE隧道

通用路由选择封装（GRE）最初是由Cisco开发的，后被标准化为RFC 1701。RFC 1702为GRE定义了IP递送报头。两个具有IP可达性的场点之间的GRE隧道可被称为VPN，因为场点之间传输的私有数据被封装在GRE递送报头中。

Internet可能是全球覆盖范围最广的公共网络，因此可以使用GRE隧道通过它连接公司的众多场点。在这种模型中，公司的每个场点都只需要一条到Internet服务提供商的物理连接，因为场点之间的所有连接都是GRE隧道。虽然可以使用GRE通过Internet建立VPN，但由于GRE固有的风险且没有强大的安全机制，因此公司很少使用它来传输数据。

2. MPLS VPN

多协议标签交换是Cisco倡导的，最初被称为标记交换（Tag Switching），后被IETF标准化为MPLS。服务提供商们越来越多地部署MPLS，以便为客户提供MPLS VPN服务。在所有

的VPN技术中，一个通用的原则是使用递送报头对私有数据进行封装；MPLS VPN使用标签来封装原始数据（有效负载），以便在场点之间建立VPN。

注意： MPLS最常见的用途是用于创建MPLS VPN，这也是部署MPLS的主要动机；MPLS的其他用途包括使用流量工程通过MPLS提供第2层VPN服务。

RFC 2547定义了一种使用MPLS提供VPN服务的方案。相对于其他VPN技术，MPLS VPN的重要优点之一是灵活性：允许在VPN场点之间采用任何网络拓扑。例如，如果必须采用全互联配置将公司的3个场点彼此相连，使用ATM、帧中继、GRE或IPSec技术时，每个场点都必须有两条虚电路或隧道，以便连接到其他两个场点。在这种全互联配置中添加第4个场点时，每个场点都将需要3条虚电路（隧道），这需要修改每个场点的配置。如果n为VPN中的场点数，则这种模型的配置复杂度为$O(n)$，扩展复杂度为$O(n^2)$。如果通过MPLS VPN来连接3个场点，新增第4个场点时将只需修改新增场点的配置；因此，包含n个场点时，该模型的配置复杂度是常量，即O(1)。

连接MPLS VPN中的场点时没有使用点到点隧道，这使得MPLS VPN的可扩展性非常高。相对于诸如GRE等其他隧道技术，使用MPLS VPN在VPN的场点之间建立全互联连接性以及建立跨越VPN的外联网连接性很容易。MPLS VPN的缺点之一是，要连接VPN场点，这些场点处必须有服务提供商的出现点。虽然可以使用跨越Internet的GRE隧道来延伸其覆盖范围，但GRE本身的安全性非常低。第9章将讨论如何解决这种问题。

3. IPSec VPN

VPN用户关心的主要问题之一是数据通过公共网络传输的安全性。换句话说，如何在VPN中阻止他人恶意窃取数据。

保护数据的方法之一是对其进行加密。为此，可在每个场点部署加密/解密设备。IPSec是在IETF的赞助下开发的一组协议，旨在通过IP分组交换网络提供安全服务。Internet是覆盖范围最广的分组交换公共网络，因此相对于租用线VPN，通过Internet部署IPSec VPN可为公司节省更多的费用。

IPSec服务支持身份验证、完整性、访问控制和机密性。使用IPSec，可以对远程场点之间交换的信息进行加密和验证。远程接入VPN和场点到场点VPN都可以使用IPSec来部署。本章余下的内容将重点讨论IPSec协议以及使用IPSec的部署模型。

1.2.3 远程接入VPN

正如前面指出的，VPN可分为场点到场点VPN和远程接入VPN。帧中继、ATM、GRE和MPLS VPN属于场点到场点VPN，因为与场点之间的配置相关的信息是预先知道的，更重要的是，它们是静态的，不会动态地变化。另一方面，来看看需要通过Internet以VPN方式访问公司数据的远程办公人员。建立VPN连接所需的信息（如远程办公人员的IP地址）随远程办公人员的位置动态变化，VPN的另一方预先并不知道。这种VPN则归类到远程接入VPN。