CISCO

ciscopress.com

SECURITY

SSL与远程接入VPN

SSL Remote Access VPNs

An introduction to designing and configuring
SSL virtual private networks

〔美〕 Jazib Frahim, CCIE #5459
Qiang Huang, CCIE #4937 著

王喆 罗进文 白帆 译

人民邮电出版社
POSTS & TELECOM PRESS

SSL与远程接入VPN

SSL Remote Access VPNs

〔美〕 **Jazib Frahim**，CCIE #5459
Qiang Huang，CCIE #4937 著

王喆 罗进文 白帆 译

人 民 邮 电 出 版 社

北 京

图书在版编目（CIP）数据

SSL与远程接入VPN / （美）弗拉海（Frahim, J.），（美）黄（Huang, Q.）著；王喆，罗进文，白帆译. --北京：人民邮电出版社，2009.3
ISBN 978-7-115-19639-2

Ⅰ. S… Ⅱ. ①弗…②黄…③王…④罗…⑤白… Ⅲ. 计算机网络－基本知识 Ⅳ. TP393

中国版本图书馆CIP数据核字（2009）第004184号

SSL 与远程接入 VPN

◆ 著 [美] Jazib Frahim，CCIE #5459
Qiang Huang，CCIE #4937
译 王 喆 罗进文 白 帆
责任编辑 李 际
执行编辑 付 飞

◆ 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

◆ 开本：800×1000 1/16
印张：18
字数：392 千字 2009 年 3 月第 1 版
印数：1 - 3 500 册 2009 年 3 月北京第 1 次印刷

著作权合同登记号 图字：01-2008-3329 号
ISBN 978-7-115-19639-2/TP

定价：45.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

关于作者

Jazib Frahim，CCIE No. 5459，他在 Cisco 工作已有 9 年多了，拥有 Illinois 技术学院的计算机工程学士学位。起初，他在 LAN 交换小组担任 TAC 工程师，然后，又转入 TAC 安全小组担任安全产品的技术总负责人，带领一个具有 20 个工程师的小组解决复杂的安全性技术和 VPN 技术问题。现今，他是网络安全高级服务的全球安全服务实践的技术总负责人。他负责指导用户设计并实现安全的网络。他获得了路由和交换以及安全两项 CCIE 认证。他曾撰写了许多 Cisco 在线技术文档，也是 Cisco 在线论坛 NetPro 的活跃成员。他在多种场合下都是网络工作人员中的一员，也为 Cisco 用户、合作伙伴和雇员教授许多定点和在线课程。

最近，他获得了北卡罗来纳州大学的 MBA 学位。Cisco 出版的由他所著的书籍包括：Cisco Network Admission Conerol，VolumeII：NAC Deployment and Troubleshooting 及 Cisco ASA: All-in-one Firewall, IPS, and VPN Adaptive Secarity Appliance。

Qiang Huang，CCIE No.4937，是 Cisco 系统校园交换系统技术组的产品管理员，主要负责为 Cisco 市场主导模块以太网交换平台推动安全和智能业务的路标。在 Cisco 工作将近 10 年来，Qiang 是许多技术小组中的重要角色，包括：在 Cisco TAC 安全性和 VPN 小组担任技术负责人，排除安全性和 VPN 解决方案中复杂的用户部署故障；在 Cisco 高级业务组担任安全性咨询工程师，为用户提供安全状态评估和咨询服务；作为技术市场营销工程师，主要负责新兴的 SSL VPN 技术在网络安全市场中的竞争分析和市场挖掘。Qiang 在安全性和 VPN 技术方面具有广博的知识，并且具有丰富的实际用户部署经验。Qiang 获得的 CCIE 认证包括路由选择和交换、安全性和 ISP 等。他还是 Internetworking Technologies Handbook，Tourzh Edition 的主要作者。Qiang 拥有科罗拉多州大学的电子工程硕士学位。

关于技术审稿人

Pete Davis 从很小的时候就开始接触计算机和网络。在 15 岁时，他就成为了最年轻的专业网络工程师，并且是 Internet 服务提供商的第一个雇员。Pete 组建和维护着新英格兰最大的用户 Internet 服务提供商 TIAC（Internet 访问公司）的系统和网络。在 1997 年，Pete 作为一名产品专员加入了 Shiva 公司。从 1998 年开始，Pete 加入了 Altiga 网络，这是一个位于马萨诸塞州富兰克林的 VPN 承包制造厂商，在 2000 年 3 月 29 日已被 Cisco 收购。作为产品线管理者，Pete 负责推进与 VPN 相关的新产品和组件的开发。

Dave Garneau 是 Radix 集团股份有限公司的首席顾问和资深技术讲师，这个公司是一个位于亨德森和内华达州的咨询和培训公司，主要专注于网络安全性方面。作为一名顾问，Dave 专攻于 Cisco 网络安全性（包括 IronPort，现今 Cisco 的一部分）和 VPN 技术（IPSec 和 SSL VPN）。作为讲师，他在 8 个国家培训了 2500 余人，以帮助他们获得 Cisco 和 IronPort 认证。他撰写的实验室指南，在授权的 Cisco 培训合作伙伴以及出版的与网络安全相关的论文中被广泛使用。Dave 获得了以下认证：CCSP、CCNP、CCDP、CCSI、CCNA、CCDA、ICSP、ICSI 和 CNE。

献　辞

Jazib Frahim：

谨以此书献给我亲爱的妻子 Sadaf，感谢你对我的支持！

此书还要献给我的父母 Frahim 和 Perveen，感谢你们对我所有工作的鼓励和支持！

最后，我要感谢我的哥哥 Shazib 和妹妹 Erum 和 Sana、嫂子 Asiya 和我可爱的侄子 Shayan 以及我可爱的侄女 Shiza 和 Alisha。感谢你们的理解和支持！

Qiang Huang：

谨以此书献给教导我合理利用空闲时间的父母以及一直支持我的妻子！

致　　谢

感谢技术编辑 Pete Davis 和 David Garneau 对本书技术方面的贡献。他们对我们的工作进行审核，并对本书如何改进提出建议。还要感谢 Cisco 安全技术组成员 Vincent Shan、Andy Qin、James Fu 和 Awair Waheed 的帮助和指导。本书第 2 章的一些图由 Saddat Malik 提供，也对他表示感谢。需要特别感谢的是 Scott Enicke 和 Aun Raza，在最终出版之前他们对本书进行了编辑。

感谢 Cisco 出版社的这个团队，尤其是 Brett Bartow 和 Betsey Henkels，感谢他们耐心的指导和审议。他们的努力值得高度赞赏。

真诚地感谢我们的主管 Ken Cavanagh、Raj Gulani 和 Hasan Siraj 一直以来对我们的支持。

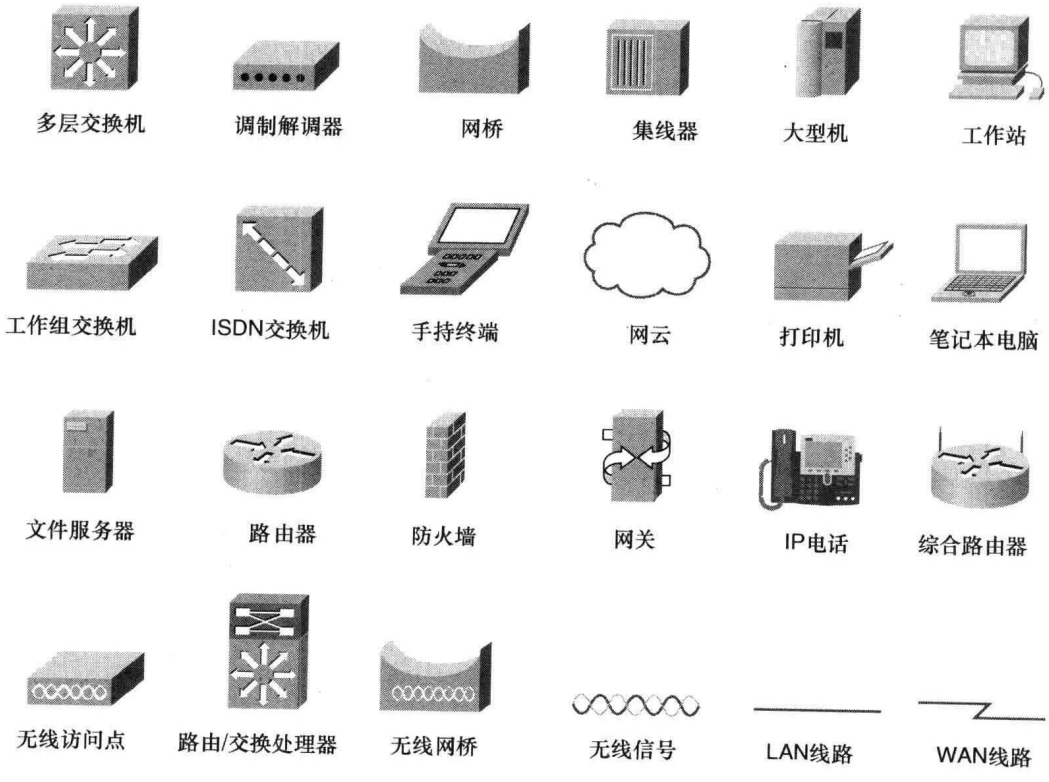
最后，感谢 Cisco TAC。在那里工作的支持 Cisco 客户的一些网络精英，经常在压力非常大的条件下创造工作奇迹。他们是真正的无名英雄，与他们并肩作战，我们感到无比荣幸。

命令语法约定

本书命令语法遵循 IOS 命令手册使用的惯例。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。

本书中使用的图标


多层交换机
调制解调器
网桥
集线器
大型机
工作站
工作组交换机
ISDN交换机
手持终端
网云
打印机
笔记本电脑
文件服务器
路由器
防火墙
网关
IP电话
综合路由器
无线访问点
路由/交换处理器
无线网桥
无线信号
LAN线路
WAN线路

前　言

本书提供了对 SSL VPN 技术的全面指导，并讨论了如何在能够使用 Cisco SSL VPN 的设备上实现 SSL VPN。设计准则能够帮助用户在现有的网络基础结构下实现 SSL VPN，包括检查现有硬件和软件以确定这些设备是否适用于 SSL VPN，提出设计建议，最后指导用户安装 Cisco SSL VPN 设备。

本书第 5 章和第 6 章的最后会介绍一些常用的部署方案，这些方案能够帮助用户在自己的网络部署 SSL VPN。

本书面向的读者

本书作为网络专业人员的指导书，旨在帮助他们在自己的网络中实现 Cisco SSL VPN 远程访问解决方案，以便用户能够方便且安全地访问企业资源。从产品或解决方案的体系结构、设备的安装、配置、部署、监视，直到 SSL VPN 解决方案的故障排除，本书将系统性地对读者进行指导。任何网络专业人员均可将此书作为在其网络中成功部署 SSL VPN 远程访问解决方案的指导书，但前提是具备 TCP/IP 和组网的基本知识并熟悉 Cisco 路由器/防火墙及其命令行界面，此外，还应对整个 SSL VPN 解决方案有一个整体的认识。

本书的结构

本书可分为 3 部分。第 1 部分包括第 1 章和第 2 章，概述了远程访问 VPN 技术，并介绍了 SSL VPN 技术。

第 2 部分包括第 3 章和第 4 章，介绍了 Cisco SSL VPN 产品系列，这些产品是基于不同设计考虑的。

第 3 部分包括第 5 章、第 6 章和第 7 章，介绍了构成 SSL VPN 解决方案的各组件的安装、配置、部署和故障排除。

- 第 1 部分包括以下两章。

  第 1 章“介绍远程访问 VPN 技术”：详细介绍了远程访问虚拟专用网（VPN，Virtual Private Network），论述了一些协议，如点对点隧道协议（PPTP，Point-to-Point Tunneling Protocol）、Internet 协议安全（IPSec，Internet Protocol Security）、第 2 层转发（L2F，Layer 2 Forwarding）、基于 IPSec 的第 2 层隧道协议（L2TP，Layer 2 Tunneling Protocol）和 SSL VPN。通过对这些协议的介绍可以使读者对可用远程访问 VPN 技术形成一个整体的概念。

第 2 章“SSL VPN 技术”：对建立 SSL VPN 的各部分进行了概述，包括加密算法、SSL 和传输层安全（TLS，Transport Layer Security）以及常用的 SSL VPN 技术。

- 第 2 部分，“SSL VPN 设计考虑事项及 Cisco 解决方案概述”包括以下两章。

第 3 章“SSL VPN 设计考虑事项”：介绍了常见设计的最佳实践，以便规划和设计一个 SSL VPN 解决方案。

第 4 章“Cisco SSL VPN 产品系列”：介绍了 Cisco 自适应安全设备（ASA，Adaptive Security Appliance）和 Cisco IOS 路由器上的 SSL VPN 功能，并主要提供了关于 SSL VPN 的产品规格说明。

- 第 3 部分，“部署 Cisco SSL VPN 解决方案”包括以下 3 章。

第 5 章“Cisco ASA 上的 SSL VPN”：详细介绍了 Cisco ASA 上的 SSL VPN 功能，还介绍了如何实现无客户端和全隧道 SSL VPN 客户端，并将重点放在 Cisco 安全桌面（CSD，Cisco Secure Desktop）上。此外，本章还介绍了用于收集终端工作站状态信息的主机扫描特性，并提供了动态访问策略（DAP，dynamic access policy）特性的用法和详细配置实例。为了加强学习，还提供了许多不同的部署方案及其配置方法。

第 6 章“Cisco IOS 路由器上的 SSL VPN”：详细介绍了 Cisco IOS 路由器上的 SSL VPN 功能。首先介绍设计准则，然后详细介绍如何配置 SSL VPN。本章还论述了如何配置无客户端、瘦客户端和 AnyConnect 客户端模式。本章后半部分的重点是 CSD，并指导如何安装 CSD 特性，为了加强学习，还给出了两个不同的部署方案及其配置方法。本章的末尾还介绍了如何通过 SDM 监视 SSL VPN。

第 7 章“管理 SSL VPN”：介绍了如何使用 Cisco 安全管理实现对 SSL VPN 的集中管理。

目　录

第1部分

介绍与技术概述

本章包括以下内容。

- IPSec
- SSL VPN
- L2TP
- 基于 IPSec 的 L2TP
- PPTP

第 1 章

介绍远程访问 VPN 技术

自从出现了 Internet，网络管理员一直在寻找利用这个廉价且被广泛使用的媒介来传输数据的方法，并且同时能保护数据的完整性和机密性。网络管理员寻找既能保护分组中信息又能为终端用户提供透明传输的方法，这便促使了虚拟专用网（VPN，Virtual Private Networks）概念的产生。后来，Internet 工程任务组（IETF，Internet Engineering Task Force）专门负责制定标准协议和规章，所有 VPN 提供商均使用这些协议和规章以保护数据机密性。

IETF 定义了许多 VPN 协议，包括点对点隧道协议（PPTP，Point-to-Point Tunneling Protocol）、第 2 层转发（L2F，Layer 2 Forwarding）、第 2 层隧道协议（L2TP，Layer 2 Tunneling Protocol）、通用路由选择封装（GRE，Generic Routing Encapsulation）、多协议标记交换（MPLS，Multiprotocol Label Switching）VPN、Internet 协议安全（IPSec，Internet Protocol Security）和安全套接字层 VPN（SSL VPN）。

VPN 协议可以明确的分为以下两组。

- 站点到站点协议。
- 远程访问协议。

站点到站点协议允许任何组织机构在两个或多个办事处之间建立安全连接，因此这种协议可利用像 Internet 这样的共享媒介传输流量。这些连接还可通过共享媒介将不同组织机构间的专用或半专用网络连接起来而无需通过租用专用线将远程办事处连接到组织机构的网络中。IPSec、GRE 和 MPLS VPN 都是常用的站点到站点 VPN 协议。