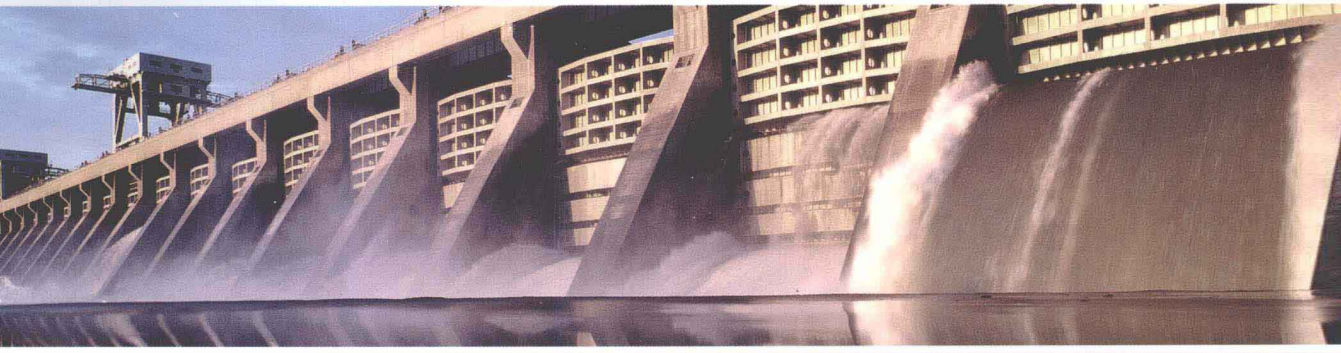
YESLAB

十年一剑

——思科安全培训领域资深讲师、
“现任明教教主”推出的**首部力作**

Cisco IPSec VPN



实战指南

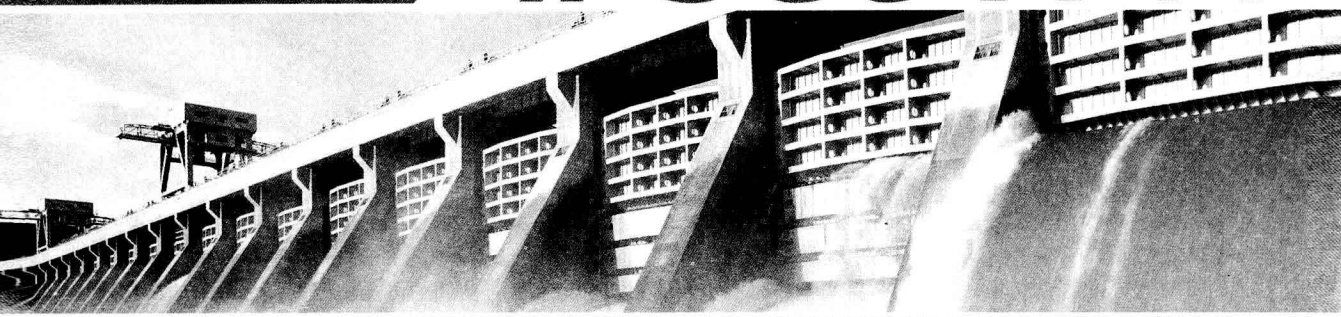
- 案例教学，分析问题，直击本质
- 独创秘籍，解决问题，另辟蹊径
- 实操性强，思科考生，必备手册

秦柯 著

人民邮电出版社
POSTS & TELECOM PRESS

YESLAB

Cisco IPSec VPN



实战指南

秦柯 著

人民邮电出版社
北京

图书在版编目（CIP）数据

Cisco IPSec VPN实战指南 / 秦柯著. -- 北京 : 人民邮电出版社, 2012.5
ISBN 978-7-115-27003-0

Ⅰ. ①C… Ⅱ. ①秦… Ⅲ. ①虚拟网络－指南 Ⅳ. ①TP393.01-62

中国版本图书馆CIP数据核字(2012)第014950号

内 容 提 要

这是一本全面介绍Cisco IPSec VPN的图书，主要涉及在Cisco路由器和ASA硬件防火墙上的IPSec VPN技术。

本书一共分为10章，分别介绍了VPN技术、GRE技术与配置、IPSec基本理论、站点到站点IPSec VPN、影响IPSec VPN的网络问题、IPSec VPN中的高可用性技术、动态多点VPN（DMVPN）、组加密传输VPN（GETVPN）、Easy VPN、ASA策略图等。本书附录还详细地介绍了Cisco模拟器的配置与使用。使用附录中介绍的模拟器可以实现本书中介绍的所有实例，因此本书的第一个特点就是实例的可操作性很强。本书的第二个特点就是采用了不同的讲述方式，作者不是生硬地介绍各种IPSec VPN特性，而是结合多年Cisco安全教学经验，首先展示各种IPSec VPN的故障现象，然后深入浅出、一步一步地分析导致这些故障的原因，最后给出相应的解决方案，让读者能够学习到整个排错和分析的过程与思路。本书的第三个特点就是大量作者原创的独门VPN解决方案，在一些特殊部署环境使用这些解决方案会得到意想不到的效果。

本书适合正在准备参加CCNA安全(640-553)、SECURE(642-637)、FIREWALL(642-617)、VPN(642-647)、CCIE安全笔试（350-018）以及CCIE安全实验考试的考生阅读，也是从事Cisco安全技术的工程师必不可少的现场参考资料。

Cisco IPSec VPN 实战指南

◆ 著　　秦　柯
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
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：21
字数：423千字　　2012年5月第1版
印数：1－3 500册　　2012年5月北京第1次印刷

ISBN 978-7-115-27003-0

定价：55.00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

秦柯，CCIE #13778，网名“现任明教教主”。于 2010 年 7 月创立 YESLAB CCIE 培训中心，是网络视频教学和网真教学的开创者之一。作者多年来一直从事网络安全、虚拟化与数据中心的教学工作，从业 10 年期间，总共培训出 300 多名 CCIE 安全学员。作者还开发了全套 CCSP、CCIE 安全、黑客技术和虚拟化与数据中心的教学资料与视频教程。这些教学资料和视频教程，得到了广大网络安全从业人员的好评。如若读者对这些资料和视频感兴趣，请通过作者的博客地址 http://blog.sina.com.cn/xrmjjz 进行查阅和下载。

献　　词

谨将本书献给我的妻子和我的父母：谢谢他们对我事业的支持，以及长期以来在生活上对我的照顾和关怀。

致　　谢

在本书的创作过程中，得到了 YesLab 实验室各位老师的大力帮助，在此表示感谢。尤其感谢 YesLab 安全团队的张雷、戴鑫和马海波老师对实验室的尽心管理，使我能够投入地创作这本书。没有你们的努力，YesLab 实验室和我都不会有今天的成绩。谢谢你们！

前　言

知行合一是几百年前明朝思想家王阳明首先提出的一种哲学思想，我认为在我们学习网络的时候，可以这样来理解知行合一的思想，“知”也就是理论知识，是我们行动的指导，没有理论的支撑，我们的行动会变得盲目，并且会走很多弯路。但是，“行”也很重要，对网络技术的学习而言，“行”的本职就是做实验做项目。大量的实验与来自工程中的经验，是对“知”也即理论知识的实践。并且我们在实践中得到的经验，反过来会验证我们学习的理论知识，能够对我们的理论起着升华的作用。

现在学习网络的学员或者朋友，主要分为两类，一类是以实践为主，每天忙于各种项目的实施，当遇到问题的时候才开始看看书，或者看看视频。对于理论知识不求甚解、得过且过，以能搞定项目为第一目标。另一类则是以理论为主，天天研究各种高深理论，在与同行进行交流时，动辄就是 LSA 的几种类型、BGP 的各种选路原则，而且还动不动的对他人的理论水平评头论足，但是，他们并不了解这些理论知识在实际工程中的应用情况，甚至可以说，他们都不知道自己学习的技术到底能做些什么！

上面这两种方法虽然都是极端，但是在现实世界中却切实存在。我以为这两类学习方法都不可取，我们应该把知行合一的思想运用到网络学习中去。我们不仅仅要学习理论，更应该知道如何将学到的理论灵活运用到实际实施的项目中，并且知道这些理论到底解决了哪些实际问题。读者们在学习网络安全技术时，最能体会到这一点。有些读者在做实验时，可能会熟练进行相关配置，但是却不知道这个实验的目的是什么，其中涉及的技术到底发挥了什么作用，它们又真正解决了客户的哪些问题。而真正的技术高手不但应该知道如何配置相关实验，还应该能够将实验中所用到的技术应用到实际的工程中，以解决来自现实世界（而非实验环境）中的问题，而且他们还要基于客户的要求选择最适当、最有效的技术，只有这样，他们才称得上是对技术融会贯通，才真正称得上“高手”二字。

下面，我与读者分享一下我的学习方法，以引导大家把知行合一的思想融合到网络技术的学习中去。当然，每个人都有最适合自己的学习方法，而且我的方法也不见得能够适合所有人，但是仍然希望读者能够用来参考。我在学习时的一个最大特点就是，把学到的所有知识都实际运用起来。我的技术专长是网络安全，以前也做过很多相关的工程，现在是以培训讲师的身份在三尺讲台之上讲授网络安全知识，这在很多读者看来，我已经远离了“一线”工作，但实则不然，我仍然会注重将掌握的理论知识实施到 YesLab 的内部网络中，也可以说，YesLab 的内部网络就是我的最前线。这样，我学习过的所有安全技术都在这个内部的网络中得到了部署。通过这种部署应用，我对安全技术理论知识的理解得到了进一步提升。除了 Cisco 安全技术之外，我还在实践中掌握了包括 CheckPoint 和 Juniper 厂商在内的安全技术。而且通过横向比较这

些厂商的产品，我对它们的产品性能和优缺点也了然于胸。

当然，部署和维护这个内部网络并不轻松，网络经常被我搞得崩溃，而且每次都会让我痛不欲生。但是每当将网络重新修复之后，这种痛苦就转换为一种甘甜，如此往复，技术不断得到升华。我在讲课时经常会提到，学员在几分钟之内就轻松搞定的VPN，可能在当初花费了我两天的时间。虽然我们的处理方式都是一样的，但是我比他们知道更多错误的处理方式。这些方式尽管不正确，但是他们让我对错误产生了比较敏锐的嗅觉。我可能无法马上找到一种正确的处理方式，但是我肯定能迅速地发现一种错误方式，而这就是行动对知识的升华。而且在每一次错误发生后，我都会从一个错误的方面来验证理论知识的正确性。

当然，在学习网络时，仅有实践也是不够的，我们还需要理论知识的支撑，为此，我们需要阅读大量的技术图书（尤其推荐人民邮电出版社出版的Cisco系列的图书），而不能仅依赖于只提供问题解决方法的技术资料和视频。而只有在图书中，才会完整地包含作者对相关问题的分析，以及解决问题的思路。再就是，就某种技术而言，我们也不可能指望通阅读一本书就将其掌握，以IPSec VPN为例，我们至少要阅读3~5本书才能真正理解该技术。毕竟，不同的作者看待问题的方法和解决问题的思路是不同的，只有当从不同的角度学习、理解这个技术之后，才能对它有一个比较深刻的认识。就像诗中说的那样“横看成岭侧成峰，远近高低各不同”。

总之，无论是学习网络安全技术，还是其他技术知识，都建议读者能够切实贯彻明朝思想家王阳明先生的“知行合一”思想，将理论应用于实践，在实践中提升对理论的认识，如此循环往复，以扎实掌握技术。

本书主要内容

本书总共分为10章内容，外加1个附录。本书从加密学理论开始，分别介绍了VPN技术、GRE技术与配置、IPSec基本理论、站点到站点IPSec VPN、影响IPSec VPN的网络问题、IPSec VPN的高可用性技术、动态多点VPN（DMVPN）、组加密传输VPN（GETVPN）、Easy VPN、ASA策略图等知识。本书具有很强的实操性，书中所有的实验环境都能够使用虚拟机来搭建。并且每一个实验给出了详细的测试过程与结果，以帮助读者彻底掌握与实验相关的理论知识和技术，真正做到“知行合一”。

第1章，“VPN技术简介”，主要讲解VPN技术特点与分类。

第2章，“GRE”，主要介绍传统GRE VPN技术。

第3章，“IPSec基本理论”，讲解了IPSec的协议特点与工作原理。

第4章，“站点到站点IPSec VPN”，介绍了站点到站点IPSec VPN的架设与配置细节。

第5章，“影响IPSec VPN的网络问题”，讨论了各种网络技术对IPSec VPN的影响及其解决方案。

第 6 章，“IPSec VPN 中的高可用性技术”，讲解了 IPSec VPN 相关的冗余技术。
第 7 章，“动态多点 VPN（DMVPN）”，介绍了 Cisco 最具特色的 DMVPN 技术。
第 8 章，“组加密传输 VPN（GETVPN）”，讲解了全新的广域网加密技术 GETVPN。
第 9 章，“Easy VPN”，讲解了 Cisco 私有的远程 VPN 技术 EzVPN。
第 10 章，“ASA 策略图”，介绍了 ASA 的策略继承关系。
附录 A，“Cisco 模拟器配置指南”，介绍了本书配套模拟器的配置与使用。

本书读者对象

本书适合 Cisco 安全的初学者、希望解决实际问题的工程实施人员，以及备考 CCNP 安全认证的人员阅读。

目　录

第 1 章

VPN 技术简介

1.1 VPN 产生背景

随着时代的发展以及企业规模的发展壮大，企业网络也在不断发生变化。例如，一家总部设在北京的企业，可能会在上海、广州和深圳等地都设有分支机构，因此需要把各个分支机构连接在一起，以便共享资源、协同工作，提高工作效率。但传统的专线联网方式价格昂贵，一般中小企业难以负担。这时低成本的 VPN 技术就孕育而生了。VPN（Virtual Private Network）即虚拟专用网络，它可以利用廉价接入的公共网络（主要使用 Internet）来传输私有数据，相较于传统的专线连网方式具有成本优势，因此被很多企业和电信运营商采用。

1.2 VPN 的两种连接方式

根据客户网络接入方式的不同，VPN 技术主要分为站点到站点（Site to Site）连接方式和远程访问（Remote Access）连接方式。

1.2.1 站点到站点（Site to Site）

站点到站点连接技术是一种主要的 VPN 连接方式，主要用于公司重要站点之间的连接。如图 1-1 所示，两个站点采用 VPN 技术虚拟地连接在一起，使得它们在通信时，就像通过普通网线一样，可以访问到对方。站点到站点的 VPN 技术对于终端用户而言是透明的，即用户感觉不到 VPN 技术的存在，而是觉得相互访问的站点位于同一个内网。

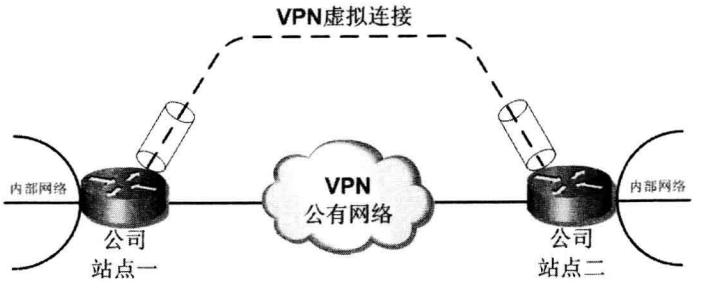


图 1-1 站点到站点 VPN 连接示意图

站点到站点 VPN 连接技术主要包括下面几种。

1. GRE

GRE（Generic Routing Encapsulation，通用路由封装）协议能够对各种网络层协议（如 IP 和 IPX）的数据报文进行封装，被封装的数据报文能够在 IP 网络中传输。GRE 采用了 Tunnel（隧道）技术，是 VPN 的三层隧道协议。由于 GRE 技术与本书重点讲解的 IPSec 技术关系紧密，所以在本书的后续部分会对 GRE 进行介绍。

2. IPSec VPN

IPsec VPN 是业界标准的网络安全协议，可以为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，从而有效地抵御网络攻击。IPSec VPN 在网络的灵活性、安全性、经济性、扩展性等方面极具优势，因此越来越受到企业用户的青睐。本书将会在后文中详细介绍 IPSec VPN 技术。

3. MPLS VPN

MPLS VPN 是指采用 MPLS 技术在宽带 IP 的骨干网络上构建企业 IP 专网，以实现跨地域、安全、高速、可靠的数据、语音、图像等多业务通信。MPLS VPN 结合区分服务、流量工程等相关技术，将公共网络可靠的性能，良好的扩展性，丰富的功能与专用网的安全、灵活、高效地结合在了一起，可以为用户提供高质量的服务。MPLS VPN 已经超出了本书的范围，感兴趣的读者可以参阅人民邮电出版社出版的《MPLS 和 VPN 体系结构》（第 1 卷、第 2 卷）等图书。

1.2.2 远程访问（Remote Access）

站点到站点 VPN 连接技术只能满足公司站点之间的连接，也就是说客户必须要在公司内部才能使用这种技术来连接其他站点。如果客户出差在外，希望在一个提供 Internet 连接的咖啡馆、飞机场或者酒店连接到公司内部，站点到站点 VPN 连接技术就不再适用了。在这种场合下，需要用到远程访问 VPN 连接技术。远程访问 VPN 一

般需要预先在客户计算机上安装 VPN 客户端（客户端依据具体采用的实现技术，而有所不同），并且通过这个客户端拨号到公司 VPN 网关。如果拨号成功，客户就像通过一根网线虚拟地连接到公司 VPN 网关，然后获取公司内部网络的一个地址，并且使用这个地址来访问公司的内部服务器，如图 1-2 所示。

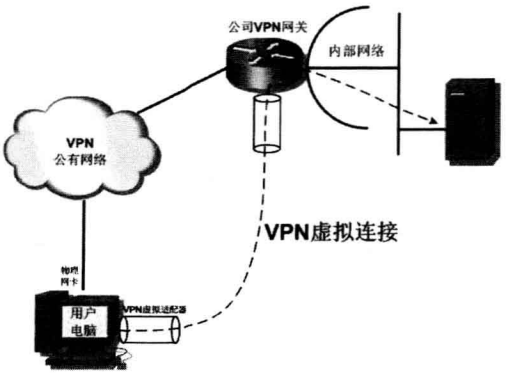


图 1-2 远程访问 VPN 示意图

远程访问 VPN 连接技术有如下几种。

1. IPSec VPN

IPSec VPN 是一种全面的技术，它不仅适用于站点到站点 VPN 连接方式，也能够部署远程访问 VPN。我们将在本书的第 8 章和第 9 章详细介绍在 Cisco 路由器和 ASA 上的 IPSec 远程访问 VPN。

2. VPDN

VPDN（Virtual Private Dial-up Networks，虚拟私有拨号网络）是 VPN 业务的一种，具体包含的技术包括 PPTP、L2TP 和 PPPoE 等，是基于拨号用户的虚拟专用拨号网业务。即用户以拨号接入方式连网，并通过 CDMA 1x 分组网络传输数据时，VPDN 会对传输的数据进行封装和加密，从而保障了传输数据的私密性，并使 VPN 达到私有网络的安全级别。VPDN 是利用 IP 网络的承载功能结合相应的认证和授权机制建立起来的一种安全的虚拟专用网，是一种比较传统的 VPN 技术。VPDN 技术已经超出了本书的内容，本书并不对此技术进行详细介绍。

3. SSL VPN

SSL VPN 指的是基于安全套接层（Security Socket Layer，SSL）协议建立远程安全访问通道的 VPN 技术。它是近年来兴起的 VPN 技术，其应用随着 Web 的普及和电子商务、远程办公的兴起而迅速发展。SSL VPN 技术已经超出了本书的内容，本书并不对此技术进行详细介绍。