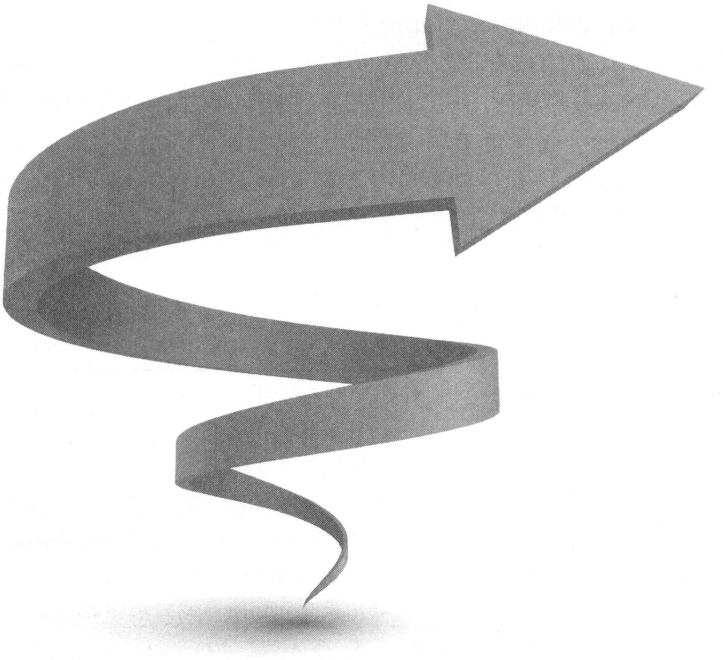
HUAWEI

“十三五”
国家重点图书出版规划项目
ICT认证系列丛书

华为技术认证

华为VPN学习指南

王 达 主编



人民邮电出版社
北 京

图书在版编目（CIP）数据

华为VPN学习指南 / 王达主编. -- 北京 : 人民邮电出版社, 2017.9
（ICT认证系列丛书）
ISBN 978-7-115-45647-2

Ⅰ. ①华… Ⅱ. ①王… Ⅲ. ①虚拟网络－指南 Ⅳ. ①TP393.01-62

中国版本图书馆CIP数据核字(2017)第165696号

内 容 提 要

本书是国内图书市场第一本，也是目前唯一一本专门介绍华为 AR 系列路由器（华为 S 系列交换机也支持部分 VPN 方案，技术原理及大多数配置方法适用于华为 NE 系列路由器和 USG 系列防火墙）IP 网络中各项 VPN 技术及应用配置的权威工具图书，同时也是华为技术有限公司指定的 ICT 认证系列培训教材。全书共 9 章，第 1 章比较全面、深入地介绍了各种 IP VPN 技术基础知识和技术原理，第 2～4 章分别介绍了 IPSec VPN 的各种技术原理，以及不同部署方式下的配置与管理方法；第 5~7 章分别介绍了 L2TP VPN、GRE VPN 和 DSVPN 的各种技术原理及配置与管理方法；第 8 章介绍了 PKI 体系架构的各种技术原理，以及不同方式下的本地数字证书的申请方法，为第 9 章采用数字证书进行身份认证的 SSL VPN 方案部署打基础；第 9 章系统地介绍了 SSL VPN 部署中有关的 SSL 策略、HTTPS 服务器，以及 SSL VPN 网关等方面的配置与管理方法。

本书结合了笔者 20 多年的工作经验，其内容非常全面、系统。为了帮助大家真正理解各项技术原理及各种 VPN 方案的配置思路，除第 1 章外，其他各章均有大量的配置示例，并对一些典型故障排除方法进行了详细的介绍。另外，本书经过了华为技术有限公司多位专家指导和审核，因此本书无论在专业性方面，还是在经验性和实用性方面均有很好的保障，是相关人员自学或者教学华为设备 VPN 配置与管理的必选教材。

◆ 主　　编　王　达
责任编辑　李　静
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　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：787×1092　1/16
印张：36.5　　2017 年 9 月第 1 版
字数：870 千字　　2017 年 9 月北京第 1 次印刷

定价：109.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

人类社会和人类文明发展的历史也是一部科学技术发展的历史。半个多世纪以来，精彩纷呈的ICT技术，汇聚成了波澜壮阔的互联网，突破了时间和空间的限制，把人类社会和人类文明带入到前所未有的高度。今天，人类社会已经步入网络和信息时代，我们已经处在无处不在的网络连接中。联接已经成为一种常态，信息浪潮迅速而深刻地改变着我们的工作和生活。人们与世界联接得如此紧密，实现了随时随地自由沟通，对信息与数据的获取、分享也唾手可得。这意味着，这个联接的世界，正以超乎想象的速度与力量，对人类社会的政治、经济、商业文明和生产方式等进行全面的重塑。

ICT正在蓬勃发展，移动化、物联网、云计算和大数据等新趋势正在引领行业开创新的格局。世界正在发生影响深远的数字化变革，互联网正在促进传统产业的升级和重构。通过以业务、用户和体验为中心的敏捷网络架构将深刻影响着未来数字社会的基础。我们深知每个人都拥有平等的数字发展机会，这对于构建一个更加公平的现实世界至关重要。

ICT产业的发展离不开人才的支撑，产业的变革也将对ICT行业人才的知识体系和综合技能提出更高的挑战。作为全球领先的信息与通信解决方案供应商，华为的产品与解决方案已广泛应用于金融、能源、交通、政府、制造等各个行业。同时，我们也非常注重对ICT专业人才的培养。所以，我们与行业专家、高校老师合作编写了“华为ICT认证系列丛书”，旨在为广大用户、ICT从业者，以及愿意投身到ICT行业中的人士提供更加便利的学习帮助。

继2014年与国内资深网络技术专家、业界知名作者王达老师合作并出版《华为交换机学习指南》《华为路由器学习指南》以来，华为ICT认证系列丛书得到广大读者的高度肯定和大力支持。随着读者朋友的成长，大家渴望更加专业的技术学习。其中在各大企业广泛使用的VPN技术，以及在各个行业广泛使用的MPLS技术就是典型代表。为此，我们再度与王达老师合作并出版《华为VPN学习指南》一书（另一本《华为MPLS学习指南》也将很快上市）。这本书从学习和实用的角度，基于学习的逻辑对知识点进行了系统地组织编排，书籍由浅入深，让读者逐步掌握各种VPN技术原理和应用方案配置与管理方法。同时该书中配备了大量不同场景下的各种VPN方案的应用配置示例和典型故障排除方法，让读者能够真正地学以致用。希望本书能够帮助读者快速地学习华为设备的VPN技术，不断提升，在ICT行业大展身手！

自　序

路漫漫其修远兮，吾将上下而求索。2017 年伊始，笔者又踏上挑战自我的漫漫征程。历经数月，终于如期、如质完成本书创作，倍感欣慰。在此要感谢我的家人对我的大力支持。

本书出版背景

自从 2014 年笔者与华为技术有限公司、人民邮电出版社合作出版了《华为交换机学习指南》和《华为路由器学习指南》图书后，许多读者一直在追问为什么没有 VPN 和 MPLS 方面的内容，尽管笔者一再向他们解释是由于篇幅实在放不下，可他们仍然希望我尽快出本专著把这两部分的内容补上。

读者的心情是可以理解的，因为目前国内图书市场上的确还没有专门介绍华为设备 VPN 和 MPLS 方面的专业图书。十多年来，笔者出版过 60 余部著作，几乎每一本都得到了读者的大力支持和高度肯定，从中可以看出，只要是用心写的好书，读者的支持是义无反顾的。这一点在三年前出版的《华为交换机学习指南》和《华为路由器学习指南》两本图书上得到了更充分的体现，因为这两本书上市三年来，一再重印（截至目前一共印刷近 30 次），并且许多培训机构和高校做了教材。

尽管如此，笔者深知要把这两部分内容写好，难度还是非常大的，因为涉及太多复杂技术原理和应用配置，而且一本书的篇幅是远远不够的。由于笔者一直都很忙，很难下这个决心。直到今年，经过近三年时间的努力，我的会员视频课程已完成过半，可以稍稍停顿一下，才正式下决心分两本书把这两部分内容给大家补上。经过与华为技术有限公司、人民邮电出版社沟通，也得到了他们各级领导的大力支持，于是就有了这两本新书的漫漫创作之路。

本书与前面出版的《华为交换机学习指南》和《华为路由器学习指南》一样，也得到了华为技术有限公司许多一线产品专家的严格审核和技术把关，提供了许多宝贵的技术指导和修订意见，还有人民邮电出版社编辑老师的多次编辑、审核，所以本书无论从专业性、实用性，还是从图书编排、出版质量上都有着非一般图书可比的全线保障，敬请大家放心选购。希望这两本书能继续得到大家的喜爱，更希望这两本书能给大家带来一些实实在在的帮助。同时也衷心地感谢华为技术有限公司和人民邮电出版社这么多位领导的大力支持，感谢各位参与本书编审的技术专家和编辑老师们的辛勤付出，你们辛苦了！

服务与支持

为了加强与读者朋友们的交流与沟通，同时也方便读者朋友们相互交流与学习，及时了解图书配套视频课程、在线培训资讯，笔者向大家提供了全方位的交流平台：

- 超级读者、学员交流 QQ 群

读者交流 QQ 群：516844263

视频课程学员 QQ 群：398772643

- 两个专家博客

51CTO 博客：http://winda.blog.51cto.com

CSDN 博客：http://blog.csdn.net/lycb_gz

- 两个认证微博

新浪微博：weibo.com/winda

腾讯微博：t.qq.com/winda2010

- 两个视频课程中心（可分期购买下载版终身会员，获得全部视频课程）

51CTO 学院课程中心：http://edu.51cto.com/lecturer/user_id-55153.html

CSDN 学院课程中心：http://edu.csdn.net/lecturer/74

- 微信及公众号

微信：windanet （加入后可拉入读者微信群）

微信公众号：windanetclass

鸣 谢

本书由王达主编并统稿，经过数十位编委、技术专家数月夜以继日地工作，一次次地严格审校、修改和完善，这本巨作终于完成，并高质量地出版上市。在此感谢华为技术有限公司各位专家慎密的技术审校和大力支持，感谢人民邮电出版社各位编辑老师，以及各位编委的辛勤工作！以下是参与本书编写和技术审校人员名单。（排名不分先后）

编委人员：何艳辉、周健辉、何江林、卢翠环、王传寿、谭文凤、李峰、郑小建、余志坚、曾育文、刘云根、谢桂安 罗广平、朱碧霞、胡海侨、黄丽君、王爽、陈玉生、蔡学军、李想、夏强、刘胜华、罗巧芬

技术审校：蓝鹏、史晓健、管超、江永红

前　言

经过数月、数十位编写、审核人员的辛勤创作和一次又一次的修改，本书终于完稿了，大家也都从这本书内容的专业性和实用性中感受到巨大的成就感。真心希望本书能给大家带来一些实际的帮助，得到大家一如既往的支持与喜爱，更诚挚欢迎、接受大家的批评与指正。

本书特色

本书在编写过程中，聚集了多位专家老师的智慧和专业技能，也权衡了各位专家老师在图书定位、内容编排、整书框架部署、以及具体的知识点写作等方面的建议。使得本书具有了许多以下鲜明特色。

（1）华为安全 HCNP 技能学习、培训的指定教材

本书由华为技术有限公司官方直接授权创作，在具体编写过程中既充分考虑了普通读者系统学习 VPN 技术及功能配置与管理方法的需求，同时也考虑到了参加华为安全 HCNP 认证考试的学习需求。本书是国内第一本、也是唯一一权威的华为网络安全领域 VPN 技术自学、培训教材。

（2）内容全面、系统、深入，一册无忧

本书是专门针对华为设备各种 IP VPN（包括 IPSec VPN、L2TP VPN、GRE VPN、DSVPN 和 SSL VPN）方案进行内容编排的，不仅介绍了各种 VPN 方案所涉及的各方面技术原理，还全面介绍了各种 VPN 在不同场景下的配置与管理方法。真正的“一册在手，别无所求”。

（3）通俗原理剖析与完善配置思路结合

为了帮助大家真正理解和掌握各种 VPN 方案的实现原理，在本书中笔者结合了近 20 年的工作和学习经验，对各种 VPN 方案所涉及的许多比较高深、复杂的技术原理进行了深入、通俗化地剖析，许多纯是经验之谈，其他渠道很难获取。另外，为了帮助大家对各种 VPN 方案在不同场景下的配置思路和方法有一个清晰的认识，笔者在内容编排上采取了分门别类的方式进行讲解，使大家可以非常快捷地找到对应场景下的完整配置思路和方法。

（4）大量配置示例和故障排除方法结合

为了增强本书的实用性，在介绍完每一种相关功能配置后都列举了大量的不同场景下的配置示例，以加深大家对前面所学技术原理和具体配置与管理方法的理解。许多配置示例完全可直接应用于不同现实场景。另外，为了使大家能在部署 VPN 方案时对所遇到的各种故障迅速地进行排除，在大部分章的最后都介绍了针对一些典型故障现象的排除方法，使得本书具有非常高的专业性和实用性。

适用读者对象

本书具备极高的系统性、专业性和实用性，适合于各层次的读者，具体如下。

- 使用华为 AR 系列路由器、USG 系列防火墙产品的用户（华为 S 系列交换机支持部分功能）；
- 华为培训合作伙伴、华为网络学院的学员；
- 高等院校的计算机网络专业学生；
- 希望从零开始系统学习华为设备 VPN 技术的读者；
- 希望有一本可在平时工作中查阅的华为设备 VPN 技术手册的读者。

本书主要内容

本书是国内图书市场中第一本专门介绍华为 VPN 技术原理及配置与管理方法的工具图书，也是华为 ICT 认证系列培训教材。全书共 9 章，以华为 AR 系列路由器（部分 VPN 方案也适用于华为 S 系列交换机，其中的技术原理及大多数配置方法同样适用于华为 USG 系列防火墙）所支持的各种 IP VPN（基于 MPLS 的 VPN 将在《华为 MPLS 学习指南》一书中介绍）方案为主线全面、系统、深入地介绍了 IPSec VPN、L2TP VPN、GRE VPN、DSVPN 和 SSL VPN 的各方面技术原理及各项功能的配置与管理方法。各章的基本内容如下。

第 1 章　VPN 基础：从宏观角度，比较全面介绍了 IP VPN 技术的一些基础知识，包括 VPN 的定义、分类、各种隧道协议（PPTP、L2TP、GRE、IPSec、MPLS），以及各种安全技术原理，包括 PAP、CHAP 身份认证原理，数据加密、数字签名、数字信封、数字证书技术原理，MD5、SHA、SM3、AES、DES 等认证或加密算法原理。

第 2 章　IPSec 基础及手工方式 IPSec VPN 配置与管理：本章首先全面、系统地介绍了 IPSec 相关的基础知识和技术原理，包括 IPSec 的安全机制、封装模式、AH 和 ESP 报头格式，IPSec 保护数据流定义方式，以及 IPSec 隧道建立原理和 IKEv1/v2 密钥交换原理。然后专门介绍采用基于 ACL 定义保护数据流的手工方式建立 IPSec 隧道的配置与管理方法。在最后介绍了在采用手工方式建立 IPSec 隧道过程中可能出现的一些典型故障的排除方法。

第 3 章　IKE 动态协商方式建立 IPSec VPN 的配置与管理：本章专门介绍了在采用基于 ACL 定义保护数据流的 IKE 协议动态协商方式建立 IPSec 隧道的配置与管理方法。本章有大量针对不同应用场景下的配置示例，并在最后也专门介绍了在采用 IKE 协议动态协商建立 IPSec 隧道的过程中可能出现的一些典型故障的排除方法。

第 4 章　基于 Tunnel 接口和 Efficient VPN 策略的 IPSec VPN 配置与管理：本章介绍了基于 Tunnel 接口定义保护数据流和基于 Efficient VPN 策略建立 IPSec 隧道的配置与管理方法。基于隧道接口方式的主要特点是无需通过 ACL 来定义数据流，凡是通过 Tunnel 接口转的数据流都将被 IPSec 保护；基于 Efficient VPN 策略方式可以使远程终端的配置极为简单，更适合采用动态 IP 公网接入的移动办公用户远程接入企业网络。

第 5 章　L2TP VPN 配置与管理：本章专门介绍了 L2TP VPN 这种二层 VPN 解决方案所涉及的各方面基础知识、技术原理和具体功能配置与管理方法。在基础方面主要包括 L2TP VPN 体系架构、L2TP 协议报文格式，L2TP 隧道模式；在技术原理方面主要涉

及 L2TP 报文的封装和传输原理、各种 L2TP 隧道模式的隧道建立流程。在本章最后列举了多个不适用不同场景下的 L2TP VPN 配置示例，介绍了在 L2TP VPN 部署中可能出现的一些典型故障的排除方法。

第 6 章　GRE VPN 配置与管理：本章专门介绍了 GRE VPN 解决方案所涉及的各方面基础知识、技术原理和具体功能配置与管理方法。主要包括 GRE 协议报文格式、GRE 报文的封装和解封装原理、GRE 安全机制和 GRE 隧道配置与管理方法。在本章最后列举了多个不适用不同场景下的 GRE VPN 配置示例，介绍了在 GRE VPN 部署中可能出现的一些典型故障的排除方法。

第 7 章　DSVPN 配置与管理：本书专门介绍了 DSVPN 解决方案所涉及的各方面基础知识、技术原理和具体功能配置与管理方法。主要包括 mGRE 协议报文的封装和解封装原理、NHRP 协议工作原理、shortcut 和非 shortcut 场景的 DSVPN 工作原理、DSVPN NAT 穿越和 IPSec 保护原理，以及 shortcut 和非 shortcut 场景下 DSVPN 隧道配置与管理方法。在本章最后列举了多个不适用不同场景、不同路由方式下的 DSVPN 配置示例，介绍了在 DSVPN 部署中可能出现的一些典型故障的排除方法。

第 8 章　PKI 配置与管理：本章是为第 9 章介绍 SSL VPN 打基础，其目的是为设备申请本地数字证书，因为在 SSL VPN 部署中要用到数字证书进行身份认证。本章主要围绕本地数字证书的申请、下载、安装、更新介绍了 PKI 各方面的基础知识、技术原理和具体功能配置与管理方法。在基础知识和技术原理方面包括 PKI 体系架构、数字证书结构和分类、PKI 工作机制。在本章最后列举了多个采用不同方式申请本地证书的配置示例，介绍了在本地证书申请过程中可能出现的一些典型故障的排除方法。

第 9 章　SSL VPN 配置与管理：本章围绕 SSL VPN 部署过程中除了 PKI 数字证书以外的 SSL 策略、HTTPS 服务器、SSL VPN 这三个方面的功能与管理方法进行介绍。部署 SSL VPN 首先要把网关设备配置为 HTTPS 服务器，以供远程用户可以通过浏览器以 Web 方式进行访问。在 HTTPS 服务器的配置过程中需要配置 SSL 服务器策略，而在创建 SSL 服务器策略时又要用到设备的本地证书。最后把设备配置为 SSL VPN 网关，为远程用户提供访问企业内网资源的 Web 页面。同样，在本章最后也列举了多个基于不同业务类型的 SSL VPN 配置示例。

阅读注意地方

在阅读本书时，请注意以下几个地方。

- 书中是以华为最新一代 AR G3 系列路由器、V200R006 及以后版本 VRP 系统的配置为主线进行介绍。
- 在配置命令代码介绍中，粗体字部分是命令本身或关键字选项部分，是不可变的；斜体字部分是命令或者关键字的参数部分，是可变的。
- 在介绍各种 VPN 技术及功能配置说明过程中，对于一些需要特别注意的地方均以粗体字格式加以强调，以便读者在阅读学习时引起特别注意。
- 为了使书中内容具有更广的适用性，在介绍具体的配置步骤过程中，对一些命令在不同 VRP 系统版本中的支持情况做了具体说明。

目　录