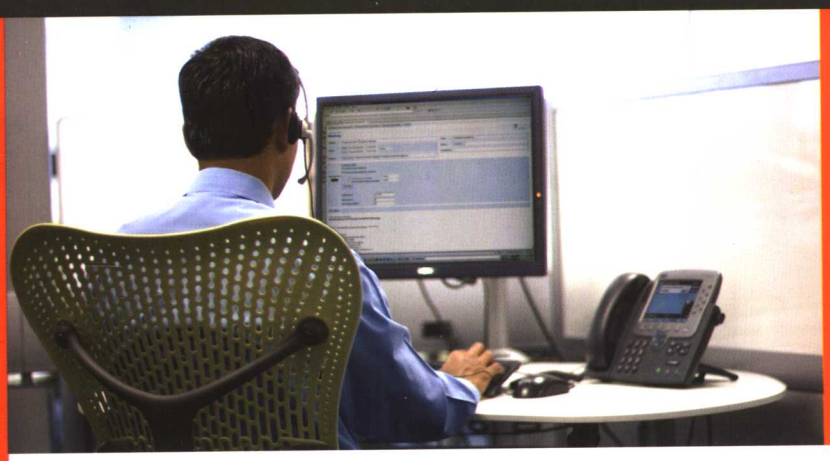
Cisco Systems

ciscopress.com

SECURITY



Cisco VPN 完全配置指南

The Complete Cisco VPN Configuration Guide

Use Cisco concentrators, routers, Cisco PIX and Cisco ASA security appliances, and remote access clients to build a complete VPN solution

[美] Richard Deal 著

姚军玲，CCIE #11470
郭稚晖 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco VPN 完全配置指南

The Complete Cisco VPN Configuration Guide

Cisco VPN 完全配置指南

[美] Richard Deal 著

姚军玲，CCIE #11470 郭稚晖 译

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

Cisco VPN 完全配置指南 /（美）迪尔（Deal,R.）著；姚军玲，郭稚晖译.
—北京：人民邮电出版社，2007.4

ISBN 978-7-115-15778-2

Ⅰ. C… Ⅱ. ①迪… ②姚… ③郭… Ⅲ. 虚拟网络—指南 Ⅳ. TP393.01-62

中国版本图书馆 CIP 数据核字（2007）第 009338 号

Cisco VPN 完全配置指南

◆ 著 [美] Richard Deal
译 姚军玲，CCIE#11470 郭稚晖
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：48.5
字数：1 224 千字 2007 年 4 月第 1 版
印数：1 – 4 000 册 2007 年 4 月北京第 1 次印刷
著作权合同登记号 图字：01-2006-4178 号
ISBN 978-7-115-15778-2/TP

定价：99.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223

前　言

多年来，Cisco 在网络行业方面一直是非常重要的组成部分，在企业网络方面还会继续扮演关键的角色。我所用的第一个路由器产品，还要追溯到 1993 年，是 Cisco 的 AGS+产品。我已经看到 IOS 的许多特色，包括您今天在 Cisco IOS 操作系统中看到的许多安全特性，例如 IPSec。在过去的几年中，我看到安全在网络设计中正在成为一种关键的要素。目前随着越来越多的公司将 Internet 作为一种业务工具，安全特别是 VPN 的使用变得越来越重要。

目标和方法

4 年前，我意识到有许多认证书籍可帮助人们通过 Cisco 的安全认证考试，然而，我发现没有任何书籍将 Cisco 的安全特性总结在一起并且应用到实际的生活场景中。我一直都在注视 Cisco 的新闻发布组，并且一直关注着如何实施各种 Cisco 安全特性方面的问题。这成为我第一本安全图书的基础，即 *Cisco PIX Fire walls*，由 McGraw-Hill/Osborne 出版。

作为一名安全方面的专家，大家总是问我一些关于设计、实施和调整 VPN 等 Cisco 产品方面的问题。因为我总是一再看到这些相同的问题，于是我决定将这些信息收集在一起，写成一本用 Cisco 产品构建 VPN 的指南。这本书的目的就是告诉读者如何使用具有 VPN 能力的 Cisco 系列产品构建 VPN，包括下面这些产品：

- IOS 路由器；
- VPN 3000 集中器；
- PIX 和 ASA 安全设备；
- VPN 3002 硬件客户端；
- Cisco VPN 客户端软件；
- Cisco SSL VPN 客户端软件；
- Microsoft 客户端软件。

因为这不是一本关于认证的图书，而是一本关于“如

何做”的图书，所以我在书中包括了下面这些方法来帮助读者实现“如何做”的过程：

- 解释什么是 VPN 以及 VPN 通常所使用的技术；
- 讨论 VPN 的实施类型，包括 IPSec，L2TP 与 PPTP，还有 SSL；
- 讨论 Cisco 具有 VPN 能力的产品及其特性和能力；
- 配置 VPN3000 集中器来实现站点到站点，或者局域网到局域网（L2L）的 VPN，还有远程访问 VPN；
- 配置 IOS 路由器来实现站点到站点和远程访问 VPN；
- 配置 PIX 和 ASA 安全设备来实现站点到站点和远程访问 VPN；
- 配置 Cisco VPN 客户端、Cisco VPN 3002 硬件客户端、Microsoft VPN Windows 客户端和 Cisco SSL 客户端来实现远程访问 VPN；
- 对 Cisco 产品常见的 VPN 问题作故障诊断与排除；
- 提供了许多例子，包括本书末尾的一个详细案例研究，通过这些例子来告诉用户如何实施 Cisco 的安全特性；
- 向用户介绍了实际生活场景中我已经处理的在实施和故障诊断与排除过程中的一些 VPN 案例——每一章都有一段见闻，说明我本人的经历。

读者对象

本书的主要目的就是提供用 Cisco 产品实施 VPN 的必要的框架。请记住，这是一本关于“如何做”的图书。虽然通过使用本书，其他的目标也可以完成，包括准备其他 Cisco 的 CCSP SNRS、SNPA、CSVPN 和 SND 的考试，但写这本书时头脑中的主要目的是：如何用具有 VPN 能力的 Cisco 产品实施 VPN。

本书假设您已具备下面这些基本知识：

- Cisco 的路由器和 IOS 操作系统与命令行接口（CLI）；
- Cisco 的 PIX 与 ASA 安全设备，和 Finesse 操作系统及其 CLI。

我在本书中所讨论的其他 Cisco 产品，例如 VPN3000 集中器，则假设读者知之甚少。然而，我会假设您对 Cisco 的产品有中级到高级的知识，至少，应当具有 Cisco CCNA 的认证来理解并且更好的使用在本书中提供的资料。

本书主要致力于使用 VPN 在设备之间或者网络之间提供安全的连接，对于当前必须使用 Cisco 产品实施 VPN 的任何网络管理员或者工程师而言都是非常有用的。

本书组织结构

本书可以逐页阅读，也可灵活使用，读者可在各章之间、每章的各节之间随意翻阅，只查找您感兴趣的资料。不过，每一部分和每一部分的每一章，都以其他部分或章节为基础。除去本书正文前面的内容外，本书共分 6 个部分。每一部分涉及 Cisco 产品的一个重要的 VPN 组件。本书各章涵盖的主题如下：

- **第 1 章，“VPN 概述”**——这一章包括一个简短的概述，论及在没有保护的网络中传输流量时所遇到外部的各种威胁，以及如何利用 VPN 保证流量的安全。这一章首先讨论通过在没有保护的网络中传输流量时经常遇到的问题：窃听、伪装、中间人

攻击。然后，本章讨论了 VPN 如何用于抵御这些攻击。我定义了什么是 VPN 及其组成、设计、VPN 实施的类型，以及选择一个特定的 VPN 解决方案时您应当考虑的标准。

- **第 2 章，“VPN 技术”**——这一章涵盖了对于实施 VPN 技术的介绍。我经常会惊讶地发现许多网络管理员和工程师并不了解他们用来保护流量的技术。因此，这一章将使用户了解 VPN 通常所使用的是什么技术，这些技术是如何工作的。这一章论及密钥、加密、数据包验证、密钥交换和验证方法。
- **第 3 章，“IPSec”**——这一章主要讲述 VPN 实施中的最重要的技术之一：IPSec。虽然这本书着眼于选择 VPN 设备，对其进行配置与故障诊断与排除，而了解某一个特定的 VPN 如何实施对于完成刚才所提到的任务也是非常重要的。在所有我参与的 VPN 的工作中，IPSec 是最复杂的；我也想找到一本将这些内容以易于理解和阅读的方式组织在一起的书。因此，这一章将讨论组成 IPSec 的标准，构建一种安全会话的两个阶段，在两个对等体之间如何建立连接以及通常导致 IPSec 会话中断的原因，这包括地址转换和防火墙，以及对这些问题的解决方案。
- **第 4 章，“PPTP 和 L2TP”**——这一章讨论了两个常见的应用在微软的 VPN 实施方案：PPTP 和 L2TP。我讨论它们是如何实施的，并且比较这两种方案。
- **第 5 章，“SSL VPNs”**——这一章讨论了使用 SSL 来实施 VPN 的解决方案。我讨论了什么是 SSL VPN 和 3 种基本的实施方法：无客户的、thin 客户和网络客户。我也讨论了通常使用的 SSL VPN 和 Cisco 的 SSL 解决方案：WebVPN。
- **第 6 章，“集中器产品信息”**——这一章介绍了 VPN 3000 集中器，它通常用于实施远程访问 VPN。这一章讨论了集中器的型号，可以插入到机箱中的模块，在不同的软件版本中提供的特性以及对集中器的 CLI 和 GUI 的介绍。
- **第 7 章，“使用 IPSec 实现集中器的远程访问连接”**——这一章着眼于在 VPN3000 集中器上终止 IPSec 远程访问连接。本章首先讨论两种控制远程访问方法——组和用户。其次讨论了如何在集中器上终止远程访问会话。本章结尾讨论集中器上的一种新的特性——网络访问控制（NAC），这种特性可以强制远程访问客户必须满足某些条件才可以建立 VPN 的会话。
- **第 8 章，“使用 PPTP、L2TP 和 WebVPN 实现集中器远程访问连接”**——这一章着眼于在 VPN3000 集中器上使用 PPTP、L2TP 和 WebVPN 来终止远程访问会话。我通过讨论在集中器上配置 PPTP 和 L2TP 来开始本章。本章还讨论了集中器上的 WebVPN（SSL VPN）特性，主要围绕 clientless、thin client 和 SSL VPN 客户端连接等主题进行讨论。也讨论了一种新的称为 Cisco 安全桌面（CSD）的 Web VPN 特性，它可以增强 WebVPN 实施的安全特性。
- **第 9 章，“集中器站点到站点的连接”**——这一章着眼于使用 VPN 3000 集中器来终止 L2L 会话。通过讨论您必须建立的一些事情来允许 ISAKMP/IKE 阶段 1 的连接构建成功来开始本章。接着讨论了如何增加 L2L 会话，这是一个简单的过程。本章的末尾讨论了在连接站点时使用重叠的地址空间，以及集中器是如何解决这些问题的。
- **第 10 章，“集中器的管理”**——不像本书中的其他章节，我在这里讨论了集中器的某些配置和管理特性。我讨论了集中器的带宽管理特性，利用它可以控制用户、组，或者 L2L 会话可以使用的带宽的量，静态和动态的路由选择能力，冗余特性，

这包括虚拟路由器冗余协议（VRRP）和虚拟簇代理（VCA）及其管理特性和屏幕画面。

- **第 11 章，“验证和故障诊断与排除集中器的连接”**——这一章讨论如何使用集中器上的不同工具来对 VPN 的连接问题进行故障诊断与排除，这包括监控屏幕（它包括活动的和过滤的事件日志）。本章的末尾介绍了远程访问 VPN 中您通常会遇到的问题，以及如何在集中器中寻找相关的信息来故障诊断与排除这些问题。我将讨论的问题包括 ISAKMP/IKE 阶段 1 的问题，例如策略不匹配和验证问题，Cisco ISAKMP/IKE 阶段 2 的问题，例如在传输集和被保护流量上的不匹配问题。
- **第 12 章，“Cisco VPN 软件客户端”**——这一章集中在使用 Cisco 的 VPN 客户端软件来建立 IPSec 远程访问会话以支持服务器产品的连接。我讨论了客户端的特性和安装及其 GUI 接口，建立到 Easy VPN 服务器（VPN 网关）的连接，GUI 选项（包括应用程序发起，Windows 登录属性，自动发起和它的集成有状态防火墙），如何更新客户端，和使用软件客户端来对通常的问题做故障诊断与排除。
- **第 13 章，“Windows 软件客户端”**——这一章讨论了如何使用微软的 Windows VPN 客户端来建立到 Cisco VPN 网关产品的 PPTP 和 L2TP/IPSec 的会话。很明显，这不是 Cisco 的产品，然而，我在本书中讨论微软的 Windows VPN 客户端的使用，是因为它通常被用来建立到 Cisco 网关设备的 VPN。这一章讨论了客户端的配置，如何配置 VPN3000 集中器接受来自微软客户端的连接，从客户端建立连接，以及故障诊断与排除通常的客户端问题。
- **第 14 章，“3002 硬件客户端”**——这一章包括了使用 VPN 3002 硬件客户端来建立 IPSec 远程访问会话。本章讨论了客户端的型号和特性，实施选项，它的 CLI 和 GUI，使用快速配置在客户端建立一个简单的配置、验证和连接选项，及管理任务，包括升级客户端。
- **第 15 章，“路由器产品信息”**——这一章涵盖了两个主要方面：对于 VPN，路由器的部署场景和 Cisco 具有 VPN 能力的路由器产品。这里主要集中于路由器在 VPN 解决方案中的特殊能力：服务质量（QoS），数据传输和路由选择扩展性。
- **第 16 章，“路由器 ISKAMP/IKE 阶段 1 连接”**——本章主要关注于当使用 IPSec 时，对于 Cisco 路由器的 ISKAMP/IKE 阶段 1 的连接。我讨论了如何建立 ISKAMP/IKE 阶段 1 的策略来保护管理连接，如何配置设备验证，监控管理连接，以及如何将一台 Cisco 路由器配置成为一个证书颁发机构（CA）。
- **第 17 章，“路由器站点到站点连接”**——这一章着眼于在 Cisco IOS 路由器上建立 L2L IPSec 会话。我讨论了如何配置 ISAKMP/IKE 阶段 2 参数（(transform sets，crypto ACL 和 crypto maps），查看和管理您的 L2L 会话，及有关 L2L 会话的一些问题。对于覆盖的一些问题，本章讨论了某些特定问题的细节和可以在路由器上解决这些问题的特性。覆盖的问题包括迁移到 IPSec VPN 的解决方案，过滤 IPSec 流量，由于地址转换和防火墙设备导致的连接中断，在 L2L 会话上传输组播和广播流量，简化 L2L 的配置，提供对 IPSec 的冗余，以及使用动态多点 VPN （DMVPN）来将 L2L 扩展实施到非常大型的多对等体连接上。
- **第 18 章，“路由器远程访问连接”**——这一章讨论了如何使用一台 IOS 路由器来实

现远程访问的 VPN 解决方案。本章讨论了如何将路由器作为 Easy VPN 的服务器，从客户端终止 IPSec 的会话，如何将路由器作为客户端并且在 Easy VPN 服务器上终止 IPSec 的会话，如何在同一台路由器上终止 L2L 和远程访问会话，以及如何在路由器上终止 WebVPN 的客户端连接。

- **第 19 章，“故障诊断与排除路由器的连接”**——这一章着眼于在 IOS 路由器上对 IPSec 的会话进行故障诊断与排除。前两小节讨论了不同的 **show**，**debug** 和 **clear** 命令，您可以使用它们来帮助您查看并对 ISAKMP/IKE 阶段 1 和阶段 2 的连接进行故障诊断与排除。本章接着介绍了某些新的故障诊断与排除特性，包括 IPSec VPN 监控，无效的 SPI 恢复特性和清除 crypto 会话。本章末尾深入讨论了碎片及其所导致的 VPN 问题，您可以在路由器上使用工具来发现碎片的问题并处理这些问题，这些工具包括扩展 ping 命令，静态的 MTU 设置，TCP 最大段尺寸（MSS）的调整和路径 MTU 发现（PMTUD）。
- **第 20 章，“PIX 和 ASA 产品信息”**——这一章包括两个主要主题：PIX 和 ASA 对于 VPN 的部署场景，以及 Cisco PIX 和 ASA 的产品。本章着眼于对于 VPN 解决方案中 PIX 和 ASA 的特殊能力：地址转换、有状态的防火墙服务和冗余。
- **第 21 章，“PIX 和 ASA 站点到站点的连接”**——本章讨论了使用 FOS 版本 6.x 和 7.x 如何在 PIX 和 ASA 安全设备上构建 IPSec L2L 会话。我在本章开始讨论了对于管理连接和验证选项配置 ISAKMP/IKE 阶段 1 的策略。接着讨论了对于数据连接的 ISAKMP/IKE 阶段 2 参数的配置，包括 transform set、crypto ACL 和 crypto maps。本章的末尾解释了使用安全设备终止 L2L 会话的一个例子。
- **第 22 章，“PIX 和 ASA 远程访问连接”**——本章讨论了使用 FOS 版本 6.x 和 7.x 如何在 PIX 和 ASA 安全设备上构建 IPSec 远程访问会话。我在本章的开始讨论了如何将一个 6.x PIX 作为 Easy VPN 的服务器来终止一个 IPSec 远程访问会话。接着我讨论了如何配置 PIX 501 和 506E 作为硬件客户端来建立到 Easy VPN 服务器的 IPSec 会话。本章的后半部分介绍使用 FOS 7.x 的 IPSec 远程访问配置，在这里我讨论了如何将 PIX 和 ASA 配置成为 Easy VPN 的服务器。在 FOS 7.0 中添加了许多新的特性，这包括隧道组、VCA 和 WebVPN，我都会在这里讨论。
- **第 23 章，“PIX 和 ASA 连接的故障诊断与排除”**——本章讨论了在 Cisco PIX 和 ASA 安全设备上的IPSec会话的故障诊断与排除问题。集中介绍了使用不同的**show**，**debug** 和 **clear** 命令来查看并且排除 ISAKMP/IKE 阶段 1 和阶段 2 的连接问题，包括成功的和对等体建立会话的例子，及不成功的建立会话的例子。
- **第 24 章，“案例研究”**——最后一章包含一个案例研究，实施了本书前面讨论过的许多的特性。我也提供了对于一个公司在建立 VPN 连接时出现问题时的解决方案和解释。

我原来还计划在本书中论及几个其他主题，如 IOS 路由器的安全设备管理器（SDM）、PIX 与 ASA 安全设备的自适应安全设备管理器、Cisco Works VMS 的 VPN 路由器管理中心。但由于篇幅所限，我只好把内容压缩到一本书可以容纳的限度。因此本书在讨论 VPN 配置时重点关注每种产品的主要接口类型，如 IOS 路由器的 CLI。另外，本书讨论的许多故障诊断与排除主题对所有 Cisco 的 VPN 产品都适用：因此本书在某些章节有选择性地挑出了某些问题加以讨论，尽管这些问题是特定的 VPN 实施类型通常会遇到的，如 IPSec。

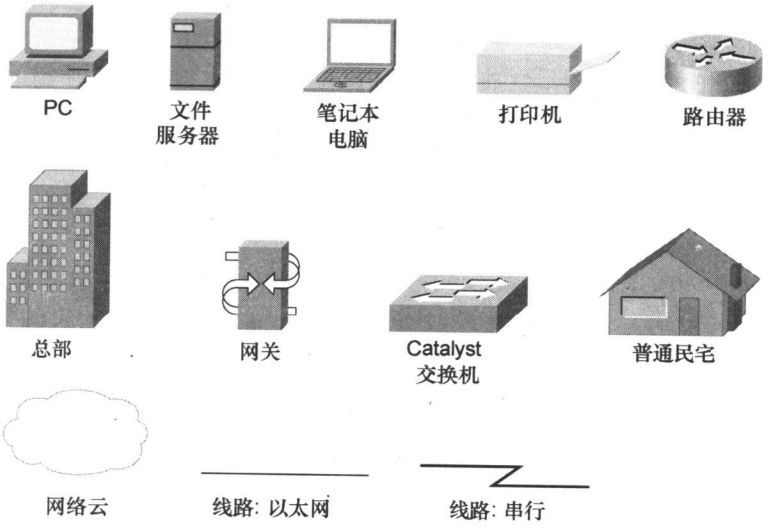
其他的信息

我在本书中讨论到的许多特性只在特定产品的不同软件版本上才被支持。为了了解某个特性是否在某个特定产品平台或者软件版本上获得支持，请用在 http://www.cisco.com/go/fn 上的 Cisco 特性导航器。您需要有一个 CCO 账户来使用这个特性。

要想了解 Cisco 产品和软件版本在产品安全建议和通知方面的列表，请浏览 http://www.cisco.com/en/US/products/products_security_advisories_listing.html。

提示：我强烈建议在您在 VPN 产品上装载某个特定的软件版本之前，先去认真地查看这个列表。

本书使用的图标



命令语法约定

本书命令语法的表示习惯和 IOS 命令参考中的表示方法是相同的。命令手册中采用如下表示方法：

- **粗体字** 代表按原样输入的命令和关键字。在实际配置的例子和输出中（非命令语法），黑体字代表用户手动输入的命令，例如 **show** 命令；
- *斜体字* 代表用户可以提供实际值的参数；
- 竖线（|）用于分开可选择的、互斥的选项；
- 方括号（ [ ]）表示可选项；
- 大括号（ { }）表示必选项；
- 方括号中的大括号（[{ }]）表示可选项中的必选项。

目　录

第一部分　VPN

第六部分 案例研究