

## <<Cisco VPN完全配置指南>>

### 图书基本信息

书名：<<Cisco VPN完全配置指南>>

13位ISBN编号：9787115293756

10位ISBN编号：7115293759

出版时间：2012-10

出版单位：人民邮电出版社

作者：迪尔

页数：756

字数：1221000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<Cisco VPN完全配置指南>>

### 内容概要

《Cisco

VPN完全配置指南》提供了VPN专家级解决方案。

全书共分为6个部分，涵盖了VPN技术的方方面面和Cisco相关产品的特性及应用。

第一部分介绍了VPN的概念及主要相关技术，包括IPSec和SSL

VPN。

第二部分详细介绍了集中器产品，并且讨论了站点到站点和远程访问的连接类型，重点在于IPSec和WebVPN。

第三部分讨论了Cisco

VPN客户端及3002硬件客户端。

第四部分介绍了Cisco

IOS路由器，讨论了可扩展的VPN，包括动态的多点VPN、路由器证书授权和路由器远程访问方案。

第五部分解释了Cisco

PIX和Cisco

ASA安全设备以及它们在VPN连接方面的作用，包括远程访问和站点到站点的连接。

第六部分通过一个案例展示了真实的VPN解决方案。

《Cisco

VPN完全配置指南》在介绍技术的同时，融入了作者的实际工作经验，并提供了故障诊断与排除方面的案例，极具参考价值。

《Cisco

VPN完全配置指南》适合想要全面、综合了解VPN技术的网络技术人员，也适合想要进一步了解网络安全核心知识的网络专业人员。

对于想参加Cisco相关认证考试的考生，本书也不失为一本很好的参考书籍。

## <<Cisco VPN完全配置指南>>

### 作者简介

Richard A. Deal在计算机与网络行业有近20年的从业经验，先后从事过网络互联、培训、系统管理与编程等工作。除了拥有格罗夫城市学院的数学与计算机科学学士学位之外，Richard还持有Cisco的多项证书。从1997年起，Richard成立了自己的公司The Deal Group, Inc。该公司位于佛罗里达州的奥兰多。在过去的8年，Richard一直在运营自己的The Deal Group Inc公司。他还在Boson Training讲授Cisco安全课程，并为其编写Cisco认证备考测试题。

## <<Cisco VPN完全配置指南>>

### 书籍目录

#### 第一部分 VPN

##### 第1章 VPN概述

###### 1.1 流量问题

###### 1.1.1 窃听攻击

###### 1.1.2 伪装攻击

###### 1.1.3 中间人攻击

###### 1.2 VPN定义

###### 1.2.1 VPN描述

###### 1.2.2 VPN连接模式

###### 1.2.3 VPN类型

###### 1.2.4 VPN分类

###### 1.3 VPN组件

###### 1.3.1 验证

###### 1.3.2 封装方法

###### 1.3.3 数据加密

###### 1.3.4 数据包的完整性

###### 1.3.5 密钥管理

###### 1.3.6 抗抵赖性

###### 1.3.7 应用程序和协议的支持

###### 1.3.8 地址管理

###### 1.4 VPN设计

###### 1.4.1 连接类型

###### 1.4.2 VPN考虑

###### 1.4.3 冗余

###### 1.5 VPN实施

###### 1.5.1 GRE

###### 1.5.2 IPSec

###### 1.5.3 PPTP

###### 1.5.4 L2TP

###### 1.5.5 MPLS

###### 1.5.6 SSL

###### 1.6 VPN：选择解决方案

###### 1.6.1 安全性

###### 1.6.2 实施、管理和支持

###### 1.6.3 高可靠性

###### 1.6.4 扩展性和灵活性

###### 1.6.5 费用

###### 1.7 总结

##### 第2章 VPN技术

###### 2.1 密钥

###### 2.1.1 密钥的使用

###### 2.1.2 对称密钥

###### 2.1.3 非对称密钥

###### 2.2 加密

###### 2.2.1 加密的过程

## <<Cisco VPN完全配置指南>>

- 2.2.2 加密算法
- 2.3 数据包验证
  - 2.3.1 数据包验证的实施
  - 2.3.2 数据包验证的使用
  - 2.3.3 数据包验证的问题
- 2.4 密钥交换
  - 2.4.1 密钥共享的困惑
  - 2.4.2 Diffie-HellMan(赫尔曼算法)
  - 2.4.3 密钥刷新
  - 2.4.4 密钥交换方法的限制
- 2.5 验证方法
  - 2.5.1 中间人攻击
  - 2.5.2 验证的解决方案
  - 2.5.3 设备验证
  - 2.5.4 用户验证
- 2.6 总结
- 第3章 IPSec
  - 3.1 IPSec标准
    - 3.1.1 IETF RFC
    - 3.1.2 IPSec连接
    - 3.1.3 构建连接的基本过程
  - 3.2 ISAKMP/IKE阶段1
    - 3.2.1 管理连接
    - 3.2.2 密钥交换协议：Diffie-Hellman
    - 3.2.3 设备验证
    - 3.2.4 远程访问额外的步骤
  - 3.3 ISAKMP/IKE阶段2
    - 3.3.1 ISAKMP/IKE阶段2组件
    - 3.3.2 阶段2安全协议
    - 3.3.3 阶段2的连接模式
    - 3.3.4 阶段2的传输集
    - 3.3.5 数据连接
  - 3.4 IPSec流量和网络
    - 3.4.1 IPSec和地址转换
    - 3.4.2 IPSec和防火墙
    - 3.4.3 使用IPSec的其他问题
  - 3.5 总结
- 第4章 PPTP和L2TP
  - 4.1 PPTP
    - 4.1.1 PPP回顾
    - 4.1.2 PPTP组件
    - 4.1.3 PPTP是如何工作的
    - 4.1.4 使用PPTP的问题
  - 4.2 L2TP
    - 4.2.1 L2TP概述
    - 4.2.2 L2TP操作
    - 4.2.3 L2TP/IPSec和PPTP的比较

## <<Cisco VPN完全配置指南>>

### 4.3 总结

## 第5章 SSL VPN

### 5.1 SSL回顾

#### 5.1.1 SSL客户实施

#### 5.1.2 SSL保护

#### 5.1.3 SSL组件

### 5.2 什么时候使用SSL VPN

#### 5.2.1 SSL VPN的好处

#### 5.2.2 SSL VPN的缺点

### 5.3 Cisco的WebVPN解决方案

#### 5.3.1 VPN 3000系列集中器

#### 5.3.2 WebVPN的操作

#### 5.3.3 Web访问

#### 5.3.4 网络浏览和文件管理访问

#### 5.3.5 应用程序访问和端口转发

#### 5.3.6 E-mail客户的访问

### 5.4 总结

## 第二部分 集中器

## 第6章 集中器产品信息

### 6.1 集中器的型号

#### 6.1.1 3005集中器

#### 6.1.2 3015集中器

#### 6.1.3 3020集中器

#### 6.1.4 3030集中器

#### 6.1.5 3060集中器

#### 6.1.6 3080集中器

#### 6.1.7 集中器型号的比较

### 6.2 集中器的模块

#### 6.2.1 SEP模块

#### 6.2.2 SEP操作

### 6.3 集中器的特性

#### 6.3.1 版本3.5特性

#### 6.3.2 版本3.6特性

#### 6.3.3 版本4.0特性

#### 6.3.4 版本4.1特性

#### 6.3.5 版本4.7特性

### 6.4 介绍对集中器的访问

#### 6.4.1 命令行接口

#### 6.4.2 图形用户接口

### 6.5 总结

## 第7章 使用IPSec实现集中器的远程访问连接

### 7.1 控制对集中器的远程访问会话

#### 7.1.1 组的配置

#### 7.1.2 用户配置

### 7.2 IPSec远程访问

#### 7.2.1 ISAKMP/IKE阶段1: IKE建议

#### 7.2.2 ISAKMP/IKE阶段1: 设备验证

## <<Cisco VPN完全配置指南>>

- 7.2.3 ISAKMP/IKE阶段1：IPSec标签
- 7.2.4 ISAKMP/IKE阶段1：Mode/Client Config标签
- 7.2.5 ISAKMP/IKE阶段1：Client FW标签
- 7.2.6 ISAKMP/IKE阶段2：数据SA
- 7.3 对于IPSec和L2TP/IPSec用户的网络访问控制(NAC)
  - 7.3.1 对于IPSec，NAC的全局配置
  - 7.3.2 NAC的组配置
- 7.4 总结
- 第8章 使用PPTP、L2TP和WebVPN实现集中器远程访问连接
  - 8.1 PPTP和L2TP远程访问
    - 8.1.1 PPTP和L2TP组配置
    - 8.1.2 PPTP全局配置
    - 8.1.3 L2TP全局配置
  - 8.2 WebVPN远程访问
    - 8.2.1 HTTPS访问
    - 8.2.2 WebVPN全局配置
    - 8.2.3 组配置
    - 8.2.4 SSL VPN客户端(SSL VPN客户端，SVC)
    - 8.2.5 用于WebVPN访问的Cisco安全桌面
  - 8.3 总结
- 第9章 集中器站点到站点的连接
  - 9.1 L2L连接例子
  - 9.2 ISAKMP/IKE阶段1准备
    - 9.2.1 现有的IKE策略
    - 9.2.2 IKE策略屏幕
  - 9.3 增加站点到站点的连接
    - 9.3.1 添加L2L会话
    - 9.3.2 完成L2L会话
    - 9.3.3 修改L2L会话
  - 9.4 地址转换和L2L会话
    - 9.4.1 介绍集中器地址转换的能力
    - 9.4.2 需要L2L地址转换的例子
    - 9.4.3 建立L2L地址转换规则
    - 9.4.4 启动L2L地址转换
  - 9.5 总结
- 第10章 集中器的管理
  - 10.1 带宽管理
    - 10.1.1 建立带宽策略
    - 10.1.2 激活带宽策略
  - 10.2 集中器上的路由选择
    - 10.2.1 静态路由选择
    - 10.2.2 RIP路由选择协议
    - 10.2.3 OSPF路由选择协议
  - 10.3 机箱冗余
    - 10.3.1 VRRP
    - 10.3.2 VCA
  - 10.4 管理屏幕

## <<Cisco VPN完全配置指南>>

- 10.4.1 Administrator Access(管理员访问)
- 10.4.2 集中器的升级
- 10.4.3 文件管理
- 10.5 总结
- 第11章 验证和故障诊断与排除集中器的连接
- 11.1 集中器的工具
- 11.1.1 系统状态
- 11.1.2 VPN会话
- 11.1.3 事件日志
- 11.1.4 监控统计信息屏幕
- 11.2 故障诊断与排除问题
- 11.2.1 ISAKMP/IKE阶段1的问题
- 11.2.2 ISAKMP/IKE阶段2的问题
- 11.3 总结
- 第三部分 客户端
- 第12章 Cisco VPN软件客户端
- 12.1 Cisco VPN客户端的概述
- 12.1.1 Cisco VPN客户端的特性
- 12.1.2 Cisco VPN客户端的安装
- 12.2 Cisco VPN客户端接口
- 12.2.1 操作模式
- 12.2.2 喜好
- 12.2.3 先进模式工具栏按钮和标签选项
- 12.3 IPSec连接
- 12.3.1 使用预共享密钥建立连接
- 12.3.2 使用证书建立连接
- 12.3.3 其他的连接配置选项
- 12.3.4 连接到一台Easy VPN服务器
- 12.3.5 客户端的连接状态
- 12.3.6 断开连接
- 12.4 VPN客户端的GUI选项
- 12.4.1 Application Launcher(应用程序发起器)
- 12.4.2 Windows Login Properties(Windows登录属性)
- 12.4.3 Automatic Initiation(自动发起)
- 12.4.4 Stateful Firewall(状态防火墙)
- 12.5 VPN客户端软件的更新
- 12.5.1 集中器：客户端更新
- 12.5.2 对于Windows 2000和XP的VPN客户端的自动更新的准备
- 12.5.3 客户端的更新过程
- 12.6 VPN客户端的故障诊断与排除
- 12.6.1 日志查看器
- 12.6.2 验证问题
- 12.6.3 ISAKMP/IKE策略不匹配的问题
- 12.6.4 地址分配的故障诊断与排除
- 12.6.5 分离隧道问题
- 12.6.6 地址转换问题
- 12.6.7 碎片问题



## <<Cisco VPN完全配置指南>>

12.6.8 Microsoft的网络邻居问题

12.7 总结

第13章 Windows软件客户端

13.1 Windows客户端

13.1.1 理解Windows客户端的特性

13.1.2 验证Windows客户端是可操作的

13.2 配置Windows VPN客户端

13.2.1 建立一个安全的策略

13.2.2 需要使用L2TP

13.2.3 建立一个Microsoft的VPN连接

13.3 配置VPN 3000集中器

13.3.1 IKE建议

13.3.2 IPSec SA

13.3.3 组配置

13.3.4 地址管理

13.3.5 用户配置

13.4 Microsoft客户端的连接

13.4.1 连接到VPN网关

13.4.2 核实PC上的连接

13.4.3 核实集中器上的连接

13.5 故障诊断与排除VPN的连接

13.5.1 集中器故障诊断与排除工具

13.5.2 Microsoft的客户端故障诊断与排除工具

13.6 总结

第14章 3002硬件客户端

14.1 3002硬件客户端概览

14.1.1 3002的特性

14.1.2 3002型号

14.1.3 3002的实施

14.2 对于3002的初始访问

14.2.1 命令行接口

14.2.2 图形用户接口

14.3 验证和连接选项

14.3.1 单元验证

14.3.2 额外的验证选项

14.4 连接模式

14.4.1 客户模式

14.4.2 网络扩展模式

14.4.3 路由和反向路由注入

14.5 管理任务

14.5.1 从公有接口上访问3002

14.5.2 升级3002

14.6 总结

第四部分 IOS路由器

第15章 路由器产品信息

15.1 路由器实施场景

15.1.1 L2L和远程访问连接

## <<Cisco VPN完全配置指南>>

- 15.1.2 路由器的特殊能力
- 15.2 路由器产品概述
- 15.3 总结
- 第16章 路由器的ISAKMP/IKE阶段1连接
  - 16.1 IPSec的准备
    - 16.1.1 收集信息
    - 16.1.2 允许IPSec的流量
  - 16.2 ISAKMP/IKE阶段1策略
    - 16.2.1 启动ISAKMP
    - 16.2.2 建立策略
    - 16.2.3 与对等体协商策略
    - 16.2.4 启动IKE死亡对等体检测
  - 16.3 ISAKMP/IKE阶段1设备验证
    - 16.3.1 ISAKMP/IKE身份类型
    - 16.3.2 预共享密钥
    - 16.3.3 RSA加密的随机数
    - 16.3.4 数字证书和路由器的注册
  - 16.4 监控和管理管理连接
    - 16.4.1 查看ISAKMP/IKE阶段1的连接
    - 16.4.2 管理ISAKMP/IKE阶段1的连接
    - 16.4.3 路由器作为证书授权
    - 16.4.4 步骤1：产生和导出RSA密钥信息
    - 16.4.5 步骤2：启动CA
    - 16.4.6 步骤3：定义额外的CA参数
    - 16.4.7 步骤4：处理申请请求
    - 16.4.8 步骤5：吊销身份证书
    - 16.4.9 步骤6：配置一台服务器使其运行在RA的模式
    - 16.4.10 步骤7：备份一个CA
    - 16.4.11 步骤8：恢复一个CA
    - 16.4.12 步骤9：清除CA服务
  - 16.5 总结
- 第17章 路由器站点到站点连接
  - 17.1 ISAKMP/IKE阶段2配置
    - 17.1.1 定义被保护的流量：Crypto ACL
    - 17.1.2 定义保护方法：Transform Set(传输集)
    - 17.1.3 构建一个静态的Crypto Map条目
    - 17.1.4 构建一个动态的Crypto Map
    - 17.1.5 可区分的基于名字的Crypto Map
  - 17.2 查看和管理连接
    - 17.2.1 查看IPSec的数据SA
    - 17.2.2 管理IPSec数据SA
  - 17.3 站点到站点连接的问题
    - 17.3.1 迁移到一个基于IPSec的设计
    - 17.3.2 过滤IPSec的流量
    - 17.3.3 地址转换和状态防火墙
    - 17.3.4 非单播流量
    - 17.3.5 配置简化

## <<Cisco VPN完全配置指南>>

- 17.3.6 IPsec冗余
- 17.3.7 L2L扩展性
- 17.4 总结
- 第18章 路由器远程访问连接
  - 18.1 Easy VPN服务器
    - 18.1.1 Easy VPN服务器的配置
    - 18.1.2 VPN组监控
    - 18.1.3 Easy VPN服务器配置例子
  - 18.2 Easy VPN远端
    - 18.2.1 Easy VPN远端连接模式
    - 18.2.2 Easy VPN远端配置
    - 18.2.3 Easy VPN远端配置的例子
  - 18.3 在同一路由器上的IPsec远程访问和L2L会话
    - 18.3.1 中心办公室路由器的配置
    - 18.3.2 远程访问和L2L样例配置
  - 18.4 WebVPN
    - 18.4.1 WebVPN建立
    - 18.4.2 WebVPN配置例子
  - 18.5 总结
- 第19章 路由器连接的故障诊断与排除
  - 19.1 ISAKMP/IKE阶段1连接
    - 19.1.1 阶段1命令的回顾
    - 19.1.2 show crypto isakmp sa命令
    - 19.1.3 debug crypto isakmp命令
    - 19.1.4 debug crypto pki命令
    - 19.1.5 debug crypto engine命令
  - 19.2 ISAKMP/IKE阶段2连接
    - 19.2.1 阶段2命令的回顾
    - 19.2.2 show crypto engine connection active命令
    - 19.2.3 show crypto ipsec sa命令
    - 19.2.4 debug crypto ipsec命令
  - 19.3 新的IPsec故障诊断与排除特性
    - 19.3.1 IPsec VPN监控特性
    - 19.3.2 清除Crypto会话
    - 19.3.3 无效的安全参数索引恢复特性
  - 19.4 碎片问题
    - 19.4.1 碎片问题
    - 19.4.2 碎片发现
    - 19.4.3 碎片问题的解决方案
  - 19.5 总结
- 第五部分 PIX防火墙
- 第20章 PIX和ASA产品信息
  - 20.1 PIX实施场景
    - 20.1.1 L2L和远程访问连接
    - 20.1.2 PIX和ASA的特殊能力
  - 20.2 PIX和ASA的特性和产品回顾
    - 20.2.1 PIX和ASA VPN特性

## <<Cisco VPN完全配置指南>>

20.2.2 PIX型号

20.2.3 ASA型号

20.3 总结

第21章 PIX和ASA站点到站点的连接

21.1 ISAKMP/IKE阶段1管理连接

21.1.1 允许IPSec的流量

21.1.2 建立ISAKMP

21.1.3 配置管理连接的策略

21.1.4 配置设备验证

21.2 ISAKMP/IKE阶段2数据连接

21.2.1 指定被保护的流量

21.2.2 定义如何保护流量

21.2.3 构建Crypto Map

21.2.4 激活一个Crypto Map

21.2.5 数据连接管理命令

21.3 L2L连接例子

21.3.1 FOS 6.3 L2L的例子

21.3.2 FOS 7.0 L2L的例子

21.4 总结

第22章 PIX和ASA远程访问连接

22.1 6.x对于Easy VPN服务器的支持

22.1.1 6.x的Easy VPN服务器的配置

22.1.2 6.x的Easy VPN服务器的例子

22.2 6.x的Easy VPN远端支持

22.2.1 6.x的Easy VPN远端配置

22.2.2 使用证书作为远程访问

22.2.3 核实您的6.x远端配置和连接

22.2.4 6.x的Easy VPN远端设备的例子配置

22.3 对于7.0的Easy VPN服务器的支持

22.3.1 理解隧道组

22.3.2 定义组策略

22.3.3 建立隧道组

22.3.4 为XAUTH建立用户账号

22.3.5 远程访问会话的问题及在7.0中的解决方案

22.3.6 解释7.0的一台Easy VPN服务器配置的例子

22.4 总结

第23章 PIX和ASA连接的故障诊断与排除

23.1 ISAKMP/IKE阶段1连接

23.1.1 阶段1命令的回顾

23.1.2 show isakmp sa命令

23.1.3 debug crypto isakmp命令

23.1.4 debug crypto vpnclient命令

23.2 ISAKMP/IKE阶段2连接

23.2.1 阶段2命令的回顾

23.2.2 show crypto ipsec sa命令

23.2.3 debug crypto ipsec命令

23.3 总结

## <<Cisco VPN完全配置指南>>

### 第六部分 案例研究

#### 第24章 案例研究

##### 24.1 公司的概貌

###### 24.1.1 总部办公室

###### 24.1.2 区域办公室

###### 24.1.3 分支办公室

###### 24.1.4 远程访问用户

##### 24.2 案例研究的配置

###### 24.2.1 边缘路由器的配置

###### 24.2.2 Internet远程访问配置

###### 24.2.3 主要园区无线的配置

##### 24.3 总结

## <<Cisco VPN完全配置指南>>

### 章节摘录

版权页： 插图： 1.数字证书的定义 证书中包含的信息可以帮助验证过程。

不像预共享密钥验证方法，证书是不预先共享的。

相反，只有当设备需要和另外一方建立连接的时候，证书才被共享。

因此，最艰难的部分就是在设备上得到证书——您不需要在您的设备上配置其他对等体的证书。

一个数字证书类似于司机驾照或者是护照的电子版本；它可以用于验证一个人（或者在这个例子里，一台设备）的身份。

数字证书是基于非对称密钥的使用（公钥 / 私钥），例如RSA加密的随机数。

您会找到许多关于数字证书的内容，我将在“X.509证书”的小节中深入讨论。

然而，关于数字证书的三件重要的事情就是一台设备的身份信息、它的公钥，和用它的私钥产生的相应的签名。

因此，能够证明一台设备的身份的必要信息都存储在一个地方：它的证书。

为了验证一个远端的对等体，您只需要它的数字证书。

当然，这就出现了一个问题：您如何知道某人送给您的证书就是他说他是的证书呢？

换句话说，一个攻击者可以产生一个数字证书，然后把它发送给您，去假冒别人。

您如何能够检测到这种类型的伪装攻击呢？

在这里我在自颁发的证书和使用一个信任的第三方，称为证书颁发机构，它所提供的可信任的证书信息之间画上一道分界线。

例如，如果双方都产生其自己的自颁发证书，如果对方在假冒别人的话，您确实不能够核实对方的身份。

因此，需要一个信任的证书仓库。

这个仓库被称为证书颁发机构（CA）。

在这种情况下，CA就是一个被所有想使用证书的设备信任的一台设备。

接着，当双方彼此想建立连接的时候，使用证书验证，他们可以使用CA作为一个信任的第三方来确保没有伪装攻击发生，并且您所连接的对方确实是它说它是的设备。

我将下面的“证书颁发机构”部分深入讨论CA。

## <<Cisco VPN完全配置指南>>

### 编辑推荐

《Cisco VPN完全配置指南》是Cisco Press出版的网络安全技术系列丛书之一《Cisco VPN完全配置指南》提供专家级解决方案《Cisco VPN完全配置指南》融入作者的实际工作经验，提供故障诊断与排除方面的案例

## <<Cisco VPN完全配置指南>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>