

## <<SSL与远程接入VPN>>

### 图书基本信息

书名：<<SSL与远程接入VPN>>

13位ISBN编号：9787115196392

10位ISBN编号：7115196397

出版时间：2009-3

出版时间：人民邮电出版社

作者：（美）弗拉海，（美）黄 著，王鑫藿模追

页数：272

字数：392000

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>

## <<SSL与远程接入VPN>>

### 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，以使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。

## <<SSL与远程接入VPN>>

### 内容概要

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的设置上实现SSL VPN。

全书内容可分为3个部分，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，介绍了基于不同设计考虑的Cisco SSL VPN产品系列；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。

本书旨在为网络专业人员提供系统性的指导。

读者需要具备TCP/IP和组网的基本知识，熟悉Cisco路由器/防火墙及其命令行界面，并对整个SSL VPN解决方案有一个整体的认识。

## <<SSL与远程接入VPN>>

### 作者简介

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ZAC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 ,

## &lt;&lt;SSL与远程接入VPN&gt;&gt;

## 书籍目录

第1部分 介绍与技术概述	第1章 介绍远程访问VPN技术	1.1 远程访问VPN技术	1.2		
IPSec	1.3 SSL VPN	1.4 L2TP	1.5 基于IPSec的L2TP	1.6 PPTP	1.7
小结	第2章 SSL VPN技术	2.1 SSL VPN密码构造块	2.2 SSL和TLS	2.3 SSL	
VPN	2.4 小结	2.5 参考	第2部分 SSL VPN技术	第3章 SSL VPN设计考虑事项	
3.1 并不是所有资源访问方法均等效	3.2 用户验证和访问权限管理	3.3 安全考虑事项	3.4 设备布置	3.5 平台选项	3.6 虚拟化
3.7 高可用性	3.8 性能和可扩展性	3.9 小结	3.10 参考	第4章 Cisco SSL VPN产品系列	4.1 Cisco SSL
VPN产品组合概览	4.2 Cisco ASA 5500系列	4.3 Cisco IOS路由器	4.4 小结	第3部分 部署Cisco SSL VPN解决方案	第5章 Cisco ASA上的SSL VPN
5.1 SSL VPN设计考虑事项	5.2 SSL VPN先决条件	5.3 SSL VPN预配置指南	5.4 无客户端SSL VPN配置指南	5.5 AnyConnect VPN客户端配置指南	5.6 Cisco安全桌面
5.7 主机扫描	5.8 动态访问策略	5.9 部署方案	5.10 监视和故障排除SSL VPN	5.11 小结	
第6章 Cisco IOS路由器上的SSL VPN	6.1 SSL VPN设计考虑事项	6.2 IOS SSL VPN先决条件	6.3 IOS SSL VPN配置指南	6.4 Cisco安全桌面	6.5 部署方案
6.6 在Cisco IOS中监视SSL VPN	6.7 小结	第7章 管理SSL VPN	7.1 多设备策略设置	7.2 工作流控制与基于角色的访问控制	7.3 小结
7.4 参考					

## &lt;&lt;SSL与远程接入VPN&gt;&gt;

## 章节摘录

2. 定义预登录顺序 要配置CSD参数，选择Configuration>Remote Access VPN>Secure DesktopManager>Prelogin Policy。

用户可定义预登录顺序，CSD使用此顺序识别主机并将其匹配到合适的配置文件。若客户端的计算机匹配某个配置文件，CSD可创建一个安全桌面也可启动快取清除器。下面将分别介绍为SSL VPN用户定义配置文件以及各自策略的安全桌面管理器配置。

(1) 定义预登录策略。

在所支持的Windows、OS x和基于Linux的操作系统中，用户可定义客户端计算机连接的可能来源地。例如，若用户连接来自办公室网络、家庭办公网络甚至网吧，可为每一个设备定义一个区域并给用户提供合适的访问权限。

对于来自办公室网络的用户连接，可放心将这些主机分类到完全安全区域，且放宽到低限制环境。

对于来自家庭办公室的用户，可将其分类到较为安全的区域，并应用较严格的策略。

对用来自网吧的用户。

可将其分类到最不安全的区域，并应用最为严格的策略。

贯穿本章，将使用3种预登录位置来建立配置，如下所示。

属于企业的办公室（OfficeCorpOwned）：该位置是为那些从属于企业的IP地址建立SSL VPN隧道的工作站定义的。

此外，这些工作站必须拥有惟一的注册表设定，以识别其为属于企业的计算机。

若工作站符合该配置文件，安全桌面或快取清除器将不会被开启。

属于企业的家庭办公室（HomeCorpOwned）：该位置是为那些属于企业，但从家庭办公室建立SSL VPN隧道的用户所使用的Windows计算机定义的。

这些地址不在公司地址范围之内，但可以通过识别惟一的注册表设定将这些工作站归于企业所有。

若工作站符合该配置文件，将开启安全桌面。

网吧（InternetCaf e）：该位置是为那些不符合前面任何配置文件的计算机定义的，将开启快取清除器。

## <<SSL与远程接入VPN>>

### 编辑推荐

《SSL与远程接入VPN》中提供了对组成一个有效、安全的SSL VPN解决方案的所有组件进行理解、设计、安装、配置和故障排除所需要了解的所有内容。

理解远程访问VPN技术。

例如点对点隧道协议（PPTP）、Internet协议安全（IPSec）、第二层转发（L2F）、基IPSec的第二层隧道协议（L2TP）和SSL VPN等。

了解SSL . VPN的构造块，包括加密算法、SSL和传输层安全（TLS）。

评估常见设计的最佳实践。

规划和设计SSL VPN解决方案。

深入探讨Cisco自适应安全设备（ASA）和Cisco IOS路由器上的SSL . VPN功能。

在Cisco ASA和Cisco IOS路由器上安装并配置SSL VPN。

使用Cisco安全管理器来管理SSL VPN部署。

CISCO SSL VPN解决方案（原名为Cisco WebVPN解决方案）使任何远程用户均能通过Internet和Web浏览器访问网络资源。

基于SSL VPN的远程访问使用宽带（电缆或DSL）或ISP拨号连接建立一条穿过Internet的加密隧道。从而实现对网络资源的安全访问。

《SSL与远程接入VPN》介绍了在支持SSL VPN的Cisco设备上的SSL虚拟专网的基本工作原理。书中的设计指导能够帮助读者在现有的网络基础结构下实现SSL VPN。

包括检查现有硬件及软件以确定是否可以使用SSL VPN。

提供设计建议并指导设置Cisco SSL VPN设备。

书中还介绍了常见的部署情景。

帮助读者在自己的网络中部署SSL VPN。

<<SSL与远程接入VPN>>

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>