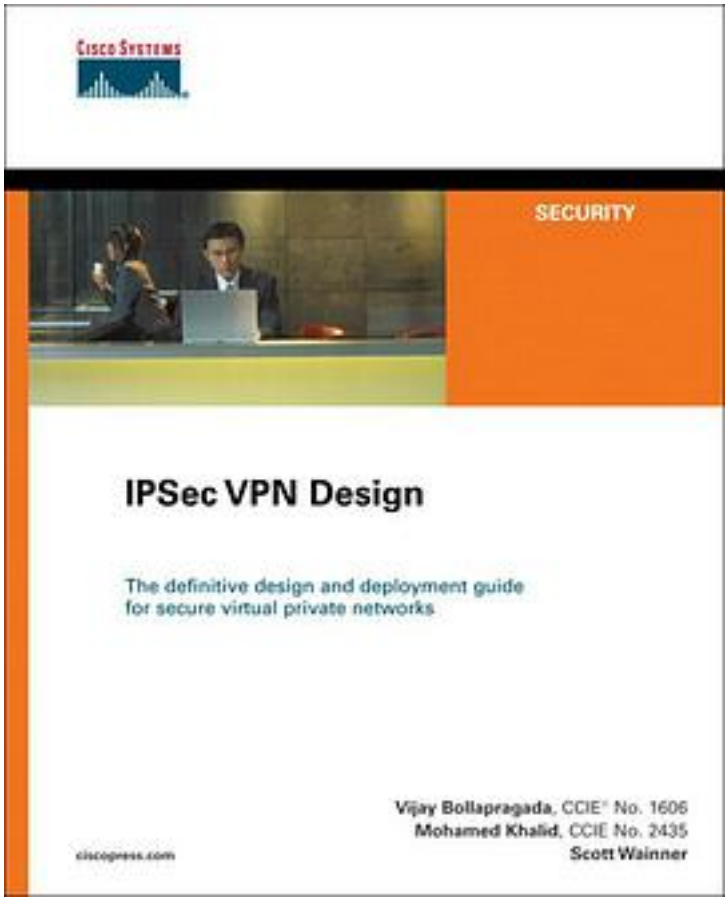
IPSec VPN Design



IPSec VPN Design_下载链接1_

著者:Bollapragada, Vijay/ Khalid, Mohamed/ Wainner, Scott

出版者:Macmillan Technical Pub

出版时间:2005-3-29

装帧:Pap

isbn:9781587051111

The definitive design and deployment guide for secure virtual private networks

Learn about IPSec protocols and Cisco IOS IPSec packet processing

Understand the differences between IPSec tunnel mode and transport mode

Evaluate the IPSec features that improve VPN scalability and fault tolerance, such as dead peer detection and control plane keepalives

Overcome the challenges of working with NAT and PMTUD

Explore IPSec remote-access features, including extended authentication, mode-configuration, and digital certificates

Examine the pros and cons of various IPSec connection models such as native IPSec, GRE, and remote access

Apply fault tolerance methods to IPSec VPN designs

Employ mechanisms to alleviate the configuration complexity of a large- scale IPSec VPN, including Tunnel End-Point Discovery (TED) and Dynamic Multipoint VPNs (DMVPN)

Add services to IPSec VPNs, including voice and multicast

Understand how network-based VPNs operate and how to integrate IPSec VPNs with MPLS VPNs

Among the many functions that networking technologies permit is the ability for organizations to easily and securely communicate with branch offices, mobile users, telecommuters, and business partners. Such connectivity is now vital to maintaining a competitive level of business productivity. Although several technologies exist that can enable interconnectivity among business sites, Internet-based virtual private networks (VPNs) have evolved as the most effective means to link corporate network resources to remote employees, offices, and mobile workers. VPNs provide productivity enhancements, efficient and convenient remote access to network resources, site-to-site connectivity, a high level of security, and tremendous cost savings.

IPSec VPN Design is the first book to present a detailed examination of the design aspects of IPSec protocols that enable secure VPN communication. Divided into three parts, the book provides a solid understanding of design and architectural issues of large-scale, secure VPN solutions. Part I includes a comprehensive introduction to the general architecture of IPSec, including its protocols and Cisco IOS® IPSec implementation details. Part II examines IPSec VPN design principles covering hub-and-spoke, full-mesh, and fault-tolerant designs. This part of the book also covers dynamic configuration models used to simplify IPSec VPN designs. Part III addresses design issues in adding services to an IPSec VPN such as voice and multicast. This part of the book also shows you how to effectively integrate IPSec VPNs with MPLS VPNs.

IPSec VPN Design provides you with the field-tested design and configuration advice to help you deploy an effective and secure VPN solution in any environment.

This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks.

作者介绍:

About the Authors

Vijay Bollapragada, CCIE No. 1606, is a director in the Network Systems Integration and Test Engineering group at Cisco Systems, where he works on the architecture, design, and validation of complex network solutions. An expert in router architecture and IP Routing, Vijay is a co-author of another Cisco Press publication titled Inside Cisco IOS Software Architecture. Vijay is also an adjunct professor in the Electrical Engineering department at Duke University.

Mohamed Khalid, CCIE No. 2435, is a technical leader working with IP VPN solutions at Cisco Systems. He works extensively with service providers across the globe and their associated Cisco account teams to determine technical and engineering requirements for various IP VPN architectures.

Scott Wainner is a Distinguished Systems Engineer in the U.S. Service Provider Sales Organization at Cisco Systems, where he focuses on VPN architecture and solution development. In this capacity, he works directly with customers in a consulting role by providing guidance on IP VPN architectures while interpreting customer requirements and driving internal development initiatives within Cisco Systems. Scott has more than 18 years of experience in the networking industry in various roles including network operations, network installation/provisioning, engineering, and product engineering. Most recently, he has focused his efforts on L2VPN and L3VPN service models using MPLS VPN, Pseudowire Emulation, and IPSec/SSL to provide VPN services to both enterprises and service providers. He holds a B.S. in Electrical Engineering from the United States Air Force Academy and a M.S. in Electronics and Computer Engineering from George Mason University in Fairfax, Virginia. Scott is currently an active member of the IEEE and the IETF.

目录: Part I, "Introduction and Concepts"
- Chapter 1, "Introduction to VPNs" Provides an introduction to VPN concepts and covers a brief introduction to various VPN technologies.
- Chapter 2, "IPSec Overview" Gives an overview of IPSec protocols and describes differences between transport mode and tunnel mode. Cisco IOS IPSec packet processing is also explained in this chapter.
- Chapter 3, "Enhanced IPSec Features" Introduces advanced IPSec features that improve IPSec VPN scalability and fault tolerance, such as dead peer detection and control plane keepalives. This chapter also explains the challenges of IPSec interoperating with Network Address Translation (NAT) and Path Maximum Transmission Unit detection (PMTUD) and how to overcome these challenges.
- Chapter 4, "IPSec Authentication and Authorization Models" Explores IPSec features that are primarily called upon for the remote access users such as Extended Authentication (XAUTH) and Mode-configuration (MODE-CFG). It also explains the Cisco EzVPN connection model and digital certificate concepts.
Part II, "Design and Deployment"
- Chapter 5, "IPSec VPN Architectures" Covers various IPSec connections models such as native IPSec, GRE, and remote access. Deployment architectures for each of the connection models are explored with pros and cons for each architecture.
- Chapter 6, "Designing Fault-Tolerant IPSec VPNs" Discusses how to introduce fault tolerance into VPN architectures and describes the caveats with the various fault-tolerance methods.
- Chapter 7, "Auto-Configuration Architectures for Site-to-Site IPSec VPNs" Covers

mechanisms to alleviate the configuration complexity of a large-scale IPSec VPN; Tunnel Endpoint Discovery (TED) and Dynamic Multipoint VPNs (DMVPN) are the two mechanisms discussed in depth.
Part III, "Service Enhancements"
- Chapter 8, "IPSec and Application Interoperability" Examines the issues with IPSec VPNs in the context of the running applications such as voice and multicast over the VPN.
- Chapter 9, "Network-Based IPSec VPNs" Concludes by introducing the concept of network-based VPNs.
・・・・・・(收起)

IPSec VPN Design_下载链接1_

标签

评论

IPSec VPN Design_下载链接1_

书评

IPSec VPN Design_下载链接1_