

## Mpls Vpn Security

Since 1993, the Information Security Management Handbook has served not only as an everyday reference for information security practitioners but also as an important document for conducting the intense review necessary to prepare for the Certified Information System Security Professional (CISSP) examination. Now completely revised and updated and in its fifth edition, the handbook maps the ten domains of the Information Security Common Body of Knowledge and provides a complete understanding of all the items in it. This is a ...must have... book, both for preparing for the CISSP exam and as a comprehensive, up-to-date reference.

End-to-End Network Security Defense-in-Depth Best practices for assessing and improving network defenses and responding to security incidents Omar Santos Information security practices have evolved from Internet perimeter protection to an in-depth defense model in which multiple countermeasures are layered throughout the infrastructure to address vulnerabilities and attacks. This is necessary due to increased attack frequency, diverse attack sophistication, and the rapid nature of attack velocity—all blurring the boundaries between the network and perimeter. End-to-End Network Security is designed to counter the new generation of complex threats. Adopting this robust security strategy defends against highly sophisticated attacks that can occur at multiple locations in your network. The ultimate goal is to deploy a set of security capabilities that together create an intelligent, self-defending network that identifies attacks as they occur, generates alerts as appropriate, and then automatically responds. End-to-End Network Security provides you with a comprehensive look at the mechanisms to counter threats to each part of your network. The book starts with a review of network security technologies then covers the six-step methodology for incident response and best practices from proactive security frameworks. Later chapters cover wireless network security, IP telephony security, data center security, and IPv6 security. Finally, several case studies representing small, medium, and large enterprises provide detailed example configurations and implementation strategies of best practices learned in earlier chapters. Adopting the techniques and strategies outlined in this book enables you to prevent day-zero attacks, improve your overall security posture, build strong policies, and deploy intelligent, self-defending networks. “Within these pages, you will find many practical tools, both process related and technology related, that you can draw on to improve your risk mitigation strategies.” —Bruce Murphy, Vice President, World Wide Security Practices, Cisco Omar Santos is a senior network security engineer at Cisco®. Omar has designed, implemented, and supported numerous secure networks for Fortune 500 companies and the U.S. government. Prior to his current role, he was a technical leader within the World Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations. Guard your network with firewalls, VPNs, and intrusion prevention systems Control network access with AAA Enforce security policies with Cisco Network Admission Control (NAC) Learn how to perform risk and threat analysis Harden your network infrastructure, security policies, and procedures against security threats Identify and classify security threats Trace back attacks to their source Learn how to best react to security incidents Maintain visibility and control over your network with the SAVE framework Apply Defense-in-Depth principles to wireless networks, IP telephony networks, data centers, and IPv6 networks 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. Category: Networking: Security Covers: Network security and incident response

All the CCNA Security 640-554 commands in one compact, portable resource Preparing for the latest CCNA® Security exam? Here are all the CCNA Security commands you need in one condensed, portable resource. Filled with valuable, easy-to-access information, the CCNA Security Portable Command Guide is portable enough for you to use whether you're in the server room or the equipment closet. Completely updated to reflect the new CCNA Security 640-554 exam, this quick reference summarizes relevant Cisco IOS® Software commands, keywords, command arguments, and associated prompts, and offers tips and examples for applying these commands to real-world security challenges. Throughout, configuration examples provide an even deeper understanding of how to use IOS to protect networks. Topics covered include

- Networking security fundamentals: concepts, policies, strategies, and more
- Securing network infrastructure: network foundations, CCP, management plane and access, and data planes (IPv6/IPv4)
- Secure connectivity: VPNs, cryptography, IPsec, and more
- Threat control and containment: strategies, ACL threat mitigation, zone-based firewalls, and Cisco IOS IPS
- Securing networks with ASA: ASDM, basic and advanced settings, and ASA SSL VPNs

Bob Vachon is a professor at Cambrian College. He has held CCNP certification since 2002 and has collaborated on many Cisco Networking Academy courses. He was the lead author for the Academy's CCNA Security v1.1 curriculum that aligns to the Cisco IOS Network Security (IINS) certification exam (640-554).

- Access all CCNA Security commands: use as a quick, offline resource for research and solutions
- Logical how-to topic groupings provide one-stop research
- Great for review before CCNA Security certification exams
- Compact size makes it easy to carry with you, wherever you go
- “Create Your Own Journal” section with blank, lined pages allows you to personalize the book for your needs
- “What Do You Want to Do?” chart inside front cover helps you to quickly reference specific tasks

This book is part of the Cisco Press® Certification Self-Study Product Family, which offers readers a self-paced study routine for Cisco® certification exams. Titles in the Cisco Press Certification Self-Study Product Family are part of a recommended learning program from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press.

This guide for network engineers describe the design, deployment, and management of Multiprotocol Label Switching (MPLS). The book explains how MPLS virtual private networks (VPNs) function and compares MPLS to other approaches. Route distribution, VPN topologies, encapsulation, label distribution, and other techniques and features are covered. Numerous charts and diagrams are featured. Tomsu is a consulting engineer. Wieser is a systems engineer. c. Book News Inc.

Theoretical and Mathematical Foundations of Computer Science

Network Security Technologies and Solutions (CCIE Professional Development Series)

The InfoSec Handbook

IPSec VPN Design

Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services

A guide to using and defining MPLS VPN services Analyze strengths and weaknesses of TDM and Layer 2 WAN services Understand the primary business and technical issues when evaluating IP/MPLS VPN offerings Describe the IP addressing, routing, load balancing, convergence, and services capabilities of the IP VPN Develop enterprise quality of service (QoS) policies and implementation guidelines Achieve scalable support for multicast services Learn the benefits and drawbacks of various security and encryption mechanisms Ensure proper use of services and plan for future growth with monitoring and reporting services Provide remote access, Internet access, and extranet connectivity to the VPN supported intranet Provide a clear and concise set of steps to plan and execute a network migration from existing ATM/Frame Relay/leased line networks to an IP VPN IP/MPLS

VPNs are compelling for many reasons. For enterprises, they enable right-sourcing of WAN services and yield generous operational cost savings. For service providers, they offer a higher level of service to customers and lower costs for service deployment. Migration comes with challenges, however. Enterprises must understand key migration issues, what the realistic benefits are, and how to optimize new services. Providers must know what aspects of their services give value to enterprises and how they can provide the best value to customers. Selecting MPLS VPN Services helps you analyze migration options, anticipate migration issues, and properly deploy IP/MPLS VPNs. Detailed configurations illustrate effective deployment while case studies present available migration options and walk you through the process of selecting the best option for your network. Part I addresses the business case for moving to an IP/MPLS VPN network, with a chapter devoted to the business and technical issues you should review when evaluating IP/MPLS VPN offerings from major providers. Part II includes detailed deployment guidelines for the technologies used in the IP/MPLS VPN. This book is part of the Networking Technology Series from Cisco Press®, which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers.

Virtual Private Networks (VPNs) are a cheap and secure way for companies to transmit information over the Internet. With implementation of two new protocols, IPsec and MPLS, VPNs are about to become standard operating procedure. This guide aims to teach network engineers and architects, internetworking pros in the enterprise and service provider organisations and security pros working on VPNs as a corporate security measure how to use them. It walks readers through a VPN build from the ground up and demonstrates how IPsec and MPLS can be used in conjunction.

MPLS VPN Security Cisco Systems

EASY-TO-FOLLOW EXAMPLES FOR SECURE, VERSATILE, COST-CUTTING, VALUE-ADDED VPNS With the security enhancements, flexibility, and market advantages now available with IPsec and MPLS, building mission-critical VPNs using these technologies has become a top agenda for many networking professionals. LEVERAGE THE BENEFITS OF IPsec AND MPLS Assembling a fully functional IPsec or MPLS VPN isn't easy. With so little information available it can be like trying to build a bicycle when you have all the components, but no idea what the final product should look like. Only Building VPNs shows, in a clear, step-by-step fashion, how to build VPNs from scratch with IPsec and MPLS. Building VPNs: With IPsec and MPLS gives you: \* From-the-ground-up directions for VPN construction \* Step-by-step implementation of IPsec for secure, inexpensive, transmission of sensitive information across the public Internet \* Easy-to-follow, diagrammed directions for deploying MPLS VPNs to provide value-added managed services \* Clear instructions for using IPsec and MPLS in the enterprise and service-provider networking environments \* Fully working solutions for both basic and advanced VPN issues \* Examples that clarify every important step in VPN design, configuration, implementation, and deployment THE BOOK TO CHOOSE FOR VPN BUILDS

Troubleshooting Virtual Private Networks  
Network Security Principles and Practices

IKEv2 IPsec Virtual Private Networks  
MPLS VPN Security

The definitive design and deployment guide for secure virtual private networks Learn about IPsec protocols and Cisco 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 tunnel mode IPsec, GRE, and remote access Apply fault tolerance methods to IPsec VPN designs Employ mechanisms to alleviate 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, 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, secure connectivity, a high level of security, and tremendous cost savings. IPsec VPN Design is the first book to present a comprehensive 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 in

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 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. & Learn the troubleshooting techniques that every IT professional running a Virtual Private Network (VPN) must master & Experience real-world solutions through practice scenarios in each chapter & An essential workplace reference for every VPN management site

The definitive guide to understanding MPLS security and implementing and operating secure MPLS networks. Understand the business case for deploying MPLS-based services and solutions \* Provides network managers and architects with a precise MPLS primer \* Defines MPLS service problems and their associated solutions \* Includes ROI models for MPLS-based solutions \* Discusses pros and cons of various options for each MPLS service Network managers often question the value that MPLS brings to their business environment. This book provides them with a precise guide for evaluating the benefits of MPLS-based applications and solutions. The book guides the network manager through the business case for MPLS by exploring other technology alternatives, including their applications, benefits, and deficiencies. Understanding the service creation process as the basis for MPLS-based solutions is pivotal when describing the benefits that MPLS offers. Furthermore, the book explores MPLS technology and its components, providing an overview of the architecture needed to reap the true advantages that MPLS brings to a service provider or enterprise network. These advantages include new revenue opportunities and a total cost of ownership reduction that positively impacts a company's bottom-line. ROI models and case study examples further confirm the business impact and help decision-makers create a blueprint for MPLS service creation. Specific aspects such as security, network management, advanced services and the future of the technology are covered in the book, helping decision makers assess MPLS as a candidate for implementation. In short, you can use this comprehensive guide to understand and build a business case for the inclusion of MPLS in your network.

Defense-in-Depth

An Introduction to Information Security

Fourth IFIP International Conference on Network Control and Engineering for QoS, Security and Mobility, Lannion, France, November 14-18, 2005

Mpls And Next-Generation Networks: Foundations For Ngn And Enterprise Virtualization

Layer 2 VPN Architectures

This volume contains the proceedings of the Fourth IFIP International Conference on Network Control and Engineering for QoS, Security and Mobility, NETCON 2005. The conference, organized by the International Federation for Information Processing, was held in Lannion, France from November 14-18, 2005. Coverage explores network security, network policy, quality of service, wireless networks, intelligent networks, and performance evaluation.

The Information Security Management Handbook continues its tradition of consistently communicating the fundamental concepts of security needed to be a true CISSP. In response to new developments, Volume 4 supplements the previous volumes with new information covering topics such as wireless, HIPAA, the latest hacker attacks and defenses, intrusion detection, and provides expanded coverage on security management issues and applications security. Even those that don't plan on sitting for the CISSP exam will find that this handbook is a great information security reference. The changes in the technology of information security and the increasing threats to security make a complete and up-to-date understanding of this material essential. Volume 4 supplements the information in the earlier volumes of this handbook, updating it and keeping it current. Organized by the ten domains of the Common Body of Knowledge (CBK) on which the CISSP exam is based, this volume gives you the information you need to understand what makes information secure and how to secure it. Because the knowledge required to master information security - the CBK - is growing so quickly, there is little duplication of material among the four volumes. As a study guide or resource that you can use on the job, the Information Security Management Handbook, Fourth Edition, Volume 4 is the book you will refer to over and over again.

Selecting MPLS VPN Services helps you analyze migration options, anticipate migration issues, and properly deploy IP/MPLS VPNs. Detailed configurations illustrate effective deployment while case studies present available migration options and walk you through the process of selecting the best option for your network. Part I addresses the business case for moving to an IP/MPLS VPN network, with a chapter devoted to the business and technical issues you should review when evaluating IP/MPLS VPN offerings from major providers. Part II includes detailed deployment guidelines for the technologies used in the IP/MPLS VPN.

Cisco Express Forwarding Understanding and troubleshooting CEF in Cisco routers and switches Nakia Stringfield, CCIE® No. 13451/Russ White, CCIE No. 2635/Stacia McKee How does a router switch a packet? What is the difference between routing a packet, switching a frame, and packet switching? What is the Cisco® Express Forwarding (CEF) feature referred to in Cisco documentation and commonly found in Cisco IOS® commands? CEF is a general term that describes the mechanism by which Cisco routers and Catalyst® switches packet-switch (route) frames. CEF is found in almost all Cisco routers and Catalyst switches, and understanding how CEF operates can improve the performance, scalability, and efficiency of your network. Cisco Express Forwarding demystifies the internal workings of Cisco routers and switches, making it easier for you to optimize performance and troubleshoot issues that arise in Cisco network environments. This book addresses common misconceptions about CEF and packet switching across various

platforms, helping you to improve your troubleshooting skills for CEF- and non-CEF-related problems. The first part of the book provides an overview of packet-switching architectures and CEF operation and advanced features. It also covers the enhanced CEF structure and general troubleshooting. The second part of the book provides case studies that focus on the common topics that have been problematic for customers and those supporting Cisco networks. Full of practical examples and configurations, this book draws on years of experience to help you keep your Cisco networks running efficiently. Learn the key features of packet-switching architectures Understand the basics of the CEF architecture and operation Examine the enhanced CEF structure, which improves scalability Learn how to troubleshoot in software-switching environments Understand the effect of CEF on a Cisco Catalyst 6500 Supervisor 720 Configure and troubleshoot load sharing with CEF Evaluate the effect of CEF in an MPLS VPN environment Review CEF design considerations that impact scalability This book is part of the Networking Technology Series from Cisco Press®, which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers. Category: Networking Covers: Routing and Switching With IPsec and MPLS Selecting MPLS VPN Services IPv6 Security CCNA Security Portable Command Guide Security Issues of MPLS Based VPN Networks

The need for information security management has never been greater. With constantly changing technology, external intrusions, and internal thefts of data, information security officers face threats at every turn. The Information Security Management Handbook on CD-ROM, 2006 Edition is now available. Containing the complete contents of the Information Security Management Handbook, this is a resource that is portable, linked and searchable by keyword. In addition to an electronic version of the most comprehensive resource for information security management, this CD-ROM contains an extra volume's worth of information that is not found anywhere else, including chapters from other security and networking books that have never appeared in the print editions. Exportable text and hard copies are available at the click of a mouse. The Handbook's numerous authors present the ten domains of the Information Security Common Body of Knowledge (CBK) ®. The CD-ROM serves as an everyday reference for information security practitioners and an important tool for any one preparing for the Certified Information System Security Professional (CISSP) ® examination. New content to this Edition: Sensitive/Critical Data Access Controls Role-Based Access Control Smartcards A Guide to Evaluating Tokens Identity Management-Benefits and Challenges An Examination of Firewall Architectures The Five "W's" and Designing a Secure Identity Based Self-Defending Network Maintaining Network Security-Availability via Intelligent Agents PBX Firewalls: Closing the Back Door Voice over WLAN Spam Wars: How to Deal with Junk E-Mail Auditing the Telephony System: Defenses against Communications Security Breaches and Toll Fraud The "Controls" Matrix Information Security Governance

Master advanced MPLS VPN deployment solutions to design, deploy, and troubleshoot advanced or large-scale networks. This title builds on the bestselling success of the first volume with more advanced features to get more out of a network.

Create and manage highly-secure Ipsec VPNs with IKEv2 and Cisco FlexVPN The IKEv2 protocol significantly improves VPN security, and Cisco's FlexVPN offers a unified paradigm and command line interface for taking full advantage of it. Simple and modular, FlexVPN relies extensively on tunnel interfaces while maximizing compatibility with legacy VPNs. Now, two Cisco network security experts offer a complete, easy-to-understand, and practical introduction to IKEv2, modern IPsec VPNs, and FlexVPN. The authors explain each key concept, and then guide you through all facets of FlexVPN planning, deployment, migration, configuration, administration, troubleshooting, and optimization. You'll discover how IKEv2 improves on IKEv1, master key IKEv2 features, and learn how to apply them with Cisco FlexVPN. IKEv2 IPsec Virtual Private Networks offers practical design examples for many common scenarios, addressing IPv4 and IPv6, servers, clients, NAT, pre-shared keys, resiliency, overhead, and more. If you're a network engineer, architect, security specialist, or VPN administrator, you'll find all the knowledge you need to protect your organization with IKEv2 and FlexVPN. Understand IKEv2 improvements: anti-DDoS cookies, configuration payloads, acknowledged responses, and more Implement modern secure VPNs with Cisco IOS and IOS-XE Plan and deploy IKEv2 in diverse real-world environments Configure IKEv2 proposals, policies, profiles, keyrings, and authorization Use advanced IKEv2 features, including SGT transportation and IKEv2 fragmentation Understand FlexVPN, its tunnel interface types, and IOS AAA infrastructure Implement FlexVPN Server with EAP authentication, pre-shared keys, and digital signatures Deploy, configure, and customize FlexVPN clients Configure, manage, and troubleshoot the FlexVPN Load Balancer Improve FlexVPN resiliency with dynamic tunnel source, backup peers, and backup tunnels Monitor IPsec VPNs with AAA, SNMP, and Syslog Troubleshoot connectivity, tunnel creation, authentication, authorization, data encapsulation, data encryption, and overlay routing Calculate IPsec overhead and fragmentation Plan your IKEv2 migration: hardware, VPN technologies, routing, restrictions, capacity, PKI, authentication, availability, and more

Master the latest MPLS VPN solutions to design, deploy, and troubleshoot advanced or large-scale networks With MPLS and VPN Architectures, Volume II, you'll learn: How to integrate various remote access technologies into the backbone providing VPN service to many different types of customers The new PE-CE routing options as well as other advanced features, including per-VPN Network Address Translation (PE-NAT) How VRFs can be extended into a customer site to provide separation inside the customer network The latest MPLS VPN security features and designs aimed at protecting the MPLS VPN backbone How to carry customer multicast traffic inside a VPN The latest inter-carrier enhancements to allow for easier and more scalable deployment of inter-carrier MPLS VPN services Advanced troubleshooting techniques including router outputs to ensure high availability MPLS and VPN Architectures, Volume II, builds on the best-selling MPLS and VPN Architectures, Volume I (1-58705-002-1), from Cisco Press. Extending into more advanced topics and deployment architectures, Volume II provides readers with the necessary tools they need to deploy and maintain a secure, highly available VPN. MPLS and VPN Architectures, Volume II, begins with a brief refresher of the MPLS VPN Architecture. Part II describes advanced MPLS VPN connectivity including the integration of service provider access technologies (dial, DSL, cable, Ethernet) and a variety of routing protocols (IS-IS, EIGRP, and OSPF), arming the reader with the knowledge of how to integrate these features into the VPN backbone. Part III details advanced deployment issues including security, outlining the necessary steps the service provider must take to protect the backbone and any attached VPN sites, and also detailing the latest security features to allow more advanced topologies and filtering. This part also covers multi-carrier MPLS VPN deployments. Finally, Part IV provides a methodology for advanced MPLS VPN troubleshooting. MPLS and VPN Architectures, Volume II, also introduces the latest advances in customer integration, security, and troubleshooting features essential to providing the advanced services based on MPLS VPN technology in a secure and scalable way. This book is part of the Networking

Technology Series from Cisco Press(r), which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers.

Information Security Management Handbook on CD-ROM, 2006 Edition

Definitive MPLS Network Designs

4th International Conference, ISA 2010, Miyazaki, Japan, June 23-25, 2010, Proceedings

Second International Conference, ICTMF 2011, Singapore, May 5-6, 2011, Revised Selected Papers

Selecting Mpls VPN Services

*Several trends are hastening the use of MPLS-based VPNs in broadband networks. With this rapid evolution, networking professionals need resources like this new volume.*

*This revised version of the bestselling first edition provides a self-study complement to the Cisco CCIP training course implementing Cisco MPLS. Extensive case studies guide readers through the design and deployment of real-world MPLS/VPN networks MPLS and VPN Architectures.*

*A guide to designing and implementing VPLS services over an IP/MPLS switched service provider backbone Today's communication providers are looking for convenience, simplicity, and flexible bandwidth across wide area networks-but with the quality of service and control that is critical for business networking applications like video, voice and data. Carrier Ethernet VPN services based on VPLS makes this a reality. Virtual Private LAN Service (VPLS) is a pseudowire (PW) based, multipoint-to-multipoint layer 2 Ethernet VPN service provided by services providers By deploying a VPLS service to customers, the operator can focus on providing high throughput, highly available Ethernet bridging services and leave the layer 3 routing decision up to the customer. Virtual Private LAN Services (VPLS) is quickly becoming the number one choice for many enterprises and service providers to deploy data communication networks. Alcatel-Lucent VPLS solution enables service providers to offer enterprise customers the operational cost benefits of Ethernet with the predictable QoS characteristics of MPLS. Items Covered: Building Converged Service Networks with IP/MPLS VPN Technology IP/MPLS VPN Multi-Service Network Overview Using MPLS Label Switched Paths as Service Transport Tunnels Routing Protocol Traffic Engineering and CSPF RSVP-TE Protocol MPLS Resiliency — Secondary LSP MPLS Resiliency — RSVP-TE LSP Fast Reroute Label Distribution Protocol IP/MPLS VPN Service Routing Architecture Virtual Leased Line Services Virtual Private LAN Service Hierarchical VPLS High Availability in an IP/MPLS VPN Network VLL Service Resiliency VPLS Service Resiliency VPLS BGP Auto-Discovery PBB-VPLS OAM in a VPLS Service Network*

*bull; Gain a comprehensive view of network security issues and concepts, then master specific implementations based on your network needs bull; Learn how to use new and legacy Cisco Systems equipment to secure your networks bull; Understand how to design and build security services while also learning the legal and network accessibility impact of those services*

*MPLS Fundamentals*

*MPLS and VPN Architectures*

*Designing Advanced Virtual Networks*

*An Advanced Guide for VPLS and VLL*

*Mpls And Vpn Architectures (Volume Ii) (642-611).*

A detailed guide for deploying PPTP, L2TPv2, L2TPv3, MPLS Layer-3, AToM, VPLS and IPSec virtual private networks.

This is the sales professional's handbook to understanding IT technologies and mastering the concepts and needs of a network environment. Essential understanding of the technologies that sales representatives need to know for success is provided here with case studies and real-world examples.

CCIE Professional Development Network Security Technologies and Solutions A comprehensive, all-in-one reference for Cisco network security Yusuf Bhaiji, CCIE No. 9305 Network Security Technologies and Solutions is a comprehensive reference to the most cutting-edge security products and methodologies available to networking professionals today. This book helps you understand and implement current, state-of-the-art network security technologies to ensure secure communications throughout the network infrastructure. With an easy-to-follow approach, this book serves as a central repository of security knowledge to help you implement end-to-end security solutions and provides a single source of knowledge covering the entire range of the Cisco network security portfolio. The book is divided into five parts mapping to Cisco security technologies and solutions: perimeter security, identity security and access management, data privacy, security monitoring, and security management. Together, all these elements enable dynamic links between customer security policy, user or host identity, and network infrastructures. With this definitive reference, you can gain a greater understanding of the solutions available and learn how to build integrated, secure networks in today's modern, heterogeneous networking environment. This book is an excellent resource for those seeking a comprehensive reference on mature and emerging security tactics and is also a great study guide for the CCIE Security exam. "Yusuf's extensive experience as a mentor and advisor in the security technology field has honed his ability to translate highly technical information into a straight-forward, easy-to-understand format. If you're looking for a truly comprehensive guide to network security, this is the one! "

-Steve Gordon, Vice President, Technical Services, Cisco Yusuf Bhaiji, CCIE No. 9305 (R&S and Security), has been with Cisco for seven years and is currently the program manager for Cisco CCIE Security certification. He is also the CCIE Proctor in the Cisco Dubai

Lab. Prior to this, he was technical lead for the Sydney TAC Security and VPN team at Cisco. Filter traffic with access lists and implement security features on switches  
 Configure Cisco IOS router firewall features and deploy ASA and PIX Firewall appliances  
 Understand attack vectors and apply Layer 2 and Layer 3 mitigation techniques  
 Secure management access with AAA Secure access control using multifactor authentication technology  
 Implement identity-based network access control  
 Apply the latest wireless LAN security solutions  
 Enforce security policy compliance with Cisco NAC  
 Learn the basics of cryptography and implement IPsec VPNs, DMVPN, GET VPN, SSL VPN, and MPLS VPN technologies  
 Monitor network activity and security incident response with network and host intrusion prevention, anomaly detection, and security monitoring and correlation  
 Deploy security management solutions such as Cisco Security Manager, SDM, ADSM, PDM, and IDM  
 Learn about regulatory compliance issues such as GLBA, HIPPA, and SOX  
 This book is part of the Cisco CCIE Professional Development Series from Cisco Press, which offers expert-level instruction on network design, deployment, and support methodologies to help networking professionals manage complex networks and prepare for CCIE exams.  
 Category: Network Security  
 Covers: CCIE Security Exam

A comprehensive introduction to all facets of MPLS theory and practice  
 Helps networking professionals choose the suitable MPLS application and design for their network  
 Provides MPLS theory and relates to basic IOS configuration examples  
 The Fundamentals Series from Cisco Press launches the basis to readers for understanding the purpose, application, and management of technologies  
 MPLS has emerged as the new networking layer for service providers throughout the world. For many service providers and enterprises MPLS is a way of delivering new applications on their IP networks, while consolidating data and voice networks. MPLS has grown to be the new default network layer for service providers and is finding its way into enterprise networks as well. This book focuses on the building blocks of MPLS (architecture, forwarding packets, LDP, MPLS and QoS, CEF, etc.). This book also reviews the different MPLS applications (MPLS VPN, MPLS Traffic Engineering, Carrying IPv6 over MPLS, AToM, VPLS, MPLS OAM etc.). You will get a comprehensive overview of all the aspects of MPLS, including the building blocks, its applications, troubleshooting and a perspective on the future of MPLS.

Information Security and Assurance  
 Securing IP Network Traffic Planes  
 Network Sales and Services Handbook  
 Information Security Management Handbook  
 Comparing, Designing, and Deploying VPNs

**IPv6 Security Protection measures for the next Internet Protocol** As the world's networks migrate to the IPv6 protocol, networking professionals need a clearer understanding of the security risks, threats, and challenges this transition presents. In **IPv6 Security**, two of the world's leading Internet security practitioners review each potential security issue introduced by IPv6 networking and present today's best solutions. **IPv6 Security** offers guidance for avoiding security problems prior to widespread IPv6 deployment. The book covers every component of today's networks, identifying specific security deficiencies that occur within IPv6 environments and demonstrating how to combat them. The authors describe best practices for identifying and resolving weaknesses as you maintain a dual stack network. Then they describe the security mechanisms you need to implement as you migrate to an IPv6-only network. The authors survey the techniques hackers might use to try to breach your network, such as IPv6 network reconnaissance, address spoofing, traffic interception, denial of service, and tunnel injection. The authors also turn to Cisco® products and protection mechanisms. You learn how to use Cisco IOS® and ASA firewalls and ACLs to selectively filter IPv6 traffic. You also learn about securing hosts with Cisco Security Agent 6.0 and about securing a network with IOS routers and switches. Multiple examples are explained for Windows, Linux, FreeBSD, and Solaris hosts. The authors offer detailed examples that are consistent with today's best practices and easy to adapt to virtually any IPv6 environment. Scott Hogg, CCIE® No. 5133, is Director of Advanced Technology Services at Global Technology Resources, Inc. (GTRI). He is responsible for setting the company's technical direction and helping it create service offerings for emerging technologies such as IPv6. He is the Chair of the Rocky Mountain IPv6 Task Force. Eric Vyncke, Cisco Distinguished System Engineer, consults on security issues throughout Europe. He has 20 years' experience in security and teaches security seminars as a guest professor at universities throughout Belgium. He also participates in the Internet Engineering Task Force (IETF) and has helped several organizations deploy IPv6 securely. Understand why IPv6 is already a latent threat in your IPv4-only network  
 Plan ahead to avoid IPv6 security problems before widespread deployment  
 Identify known areas of weakness in IPv6 security and the current state of attack tools and hacker skills  
 Understand each high-level approach to securing IPv6 and learn when to use each  
 Protect service provider networks, perimeters, LANs, and host/server connections  
 Harden IPv6 network devices against attack  
 Utilize IPsec in IPv6 environments  
 Secure mobile IPv6 networks  
 Secure transition mechanisms in use during the migration from IPv4 to IPv6  
 Monitor IPv6 security  
 Understand the security implications of the IPv6 protocol, including issues related to ICMPv6 and the IPv6 header structure  
 Protect your network against large-scale threats by using perimeter filtering techniques and service provider—focused security practices  
 Understand the vulnerabilities that exist on IPv6 access networks and learn solutions for mitigating each  
 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.  
 Category: Networking: Security  
 Covers: IPv6 Security

This book constitutes the refereed proceedings of the 5th International Conference on Distributed Computing and Internet Technology, ICDCIT 2008, held in New Delhi, India, in December 2008. The 12 revised full papers and 8 revised short papers presented were

carefully reviewed and selected from 96 submissions. Featuring current research and results in theory, methodology and applications of Distributed Computing and Internet Technology, the papers are subdivided in topical sections on distributed systems and languages, data grid, security, mobile ad-hoc networks, distributed databases, Web applications, and P2P systems.

Expert solutions for securing network infrastructures and VPNs Build security into the network by defining zones, implementing secure routing protocol designs, and building safe LAN switching environments Understand the inner workings of the Cisco PIX Firewall and analyze in-depth Cisco PIX Firewall and Cisco IOS Firewall features and concepts Understand what VPNs are and how they are implemented with protocols such as GRE, L2TP, and IPSec Gain a packet-level understanding of the IPSec suite of protocols, its associated encryption and hashing functions, and authentication techniques Learn how network attacks can be categorized and how the Cisco IDS is designed and can be set up to protect against them Control network access by learning how AAA fits into the Cisco security model and by implementing RADIUS and TACACS+ protocols Provision service provider security using ACLs, NBAR, and CAR to identify and control attacks Identify and resolve common implementation failures by evaluating real-world troubleshooting scenarios As organizations increase their dependence on networks for core business processes and increase access to remote sites and mobile workers via virtual private networks (VPNs), network security becomes more and more critical. In today's networked era, information is an organization's most valuable resource. Lack of customer, partner, and employee access to e-commerce and data servers can impact both revenue and productivity. Even so, most networks do not have the proper degree of security. Network Security Principles and Practices provides an in-depth understanding of the policies, products, and expertise that brings organization to this extremely complex topic and boosts your confidence in the performance and integrity of your network systems and services. Written by the CCIE engineer who wrote the CCIE Security lab exam and who helped develop the CCIE Security written exam, Network Security Principles and Practices is the first book to help prepare candidates for the CCIE Security exams. Network Security Principles and Practices is a comprehensive guide to network security threats and the policies and tools developed specifically to combat those threats. Taking a practical, applied approach to building security into networks, the book shows you how to build secure network architectures from the ground up. Security aspects of routing protocols, Layer 2 threats, and switch security features are all analyzed. A comprehensive treatment of VPNs and IPSec is presented in extensive packet-by-packet detail. The book takes a behind-the-scenes look at how the Cisco PIX(r) Firewall actually works, presenting many difficult-to-understand and new Cisco PIX Firewall and Cisco IOS(r) Firewall concepts. The book launches into a discussion of intrusion detection systems (IDS) by analyzing and breaking down modern-day network attacks, describing how an IDS deals with those threats in general, and elaborating on the Cisco implementation of IDS. The book also discusses AAA, RADIUS, and TACACS+ and their usage with some of the newer security implementations such as VPNs and proxy authentication. A complete section devoted to service provider techniques for enhancing customer security and providing support in the event of an attack is also included. Finally, the book concludes with a section dedicated to discussing tried-and-tested troubleshooting tools and techniques that are not only invaluable to candidates working toward their CCIE Security lab exam but also to the security network administrator running the operations of a network on a daily basis.

The InfoSec Handbook offers the reader an organized layout of information that is easily read and understood. Allowing beginners to enter the field and understand the key concepts and ideas, while still keeping the experienced readers updated on topics and concepts. It is intended mainly for beginners to the field of information security, written in a way that makes it easy for them to understand the detailed content of the book. The book offers a practical and simple view of the security practices while still offering somewhat technical and detailed information relating to security. It helps the reader build a strong foundation of information, allowing them to move forward from the book with a larger knowledge base. Security is a constantly growing concern that everyone must deal with. Whether it's an average computer user or a highly skilled computer user, they are always confronted with different security risks. These risks range in danger and should always be dealt with accordingly. Unfortunately, not everyone is aware of the dangers or how to prevent them and this is where most of the issues arise in information technology (IT). When computer users do not take security into account many issues can arise from that like system compromises or loss of data and information. This is an obvious issue that is present with all computer users. This book is intended to educate the average and experienced user of what kinds of different security practices and standards exist. It will also cover how to manage security software and updates in order to be as protected as possible from all of the threats that they face.

### Designing Network Security

#### Information Security Management Handbook, Fifth Edition

#### Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS

#### Network Control and Engineering for QoS, Security and Mobility, IV

#### MPLS-based VPNs

Field-proven MPLS designs covering MPLS VPNs, pseudowire, QoS, traffic engineering, IPv6, network recovery, and multicast Understand technology applications in various service provider and enterprise topologies via detailed design studies Benefit from the authors' vast experience in MPLS network deployment and protocol design Visualize real-world solutions through clear, detailed illustrations Design studies cover various operator profiles including an interexchange carrier (IXC), a national telco deploying a multiservice backbone carrying Internet and IP VPN services as well as national telephony traffic, an international service provider with many POPs all around the globe, and a large enterprise relying on Layer-3 VPN services to control communications within and across subsidiaries Design studies are thoroughly explained through detailed text, sample configurations, and network diagrams Definitive MPLS Network Designs provides examples of how to combine key technologies at the heart of IP/MPLS networks. Techniques are presented through a set of comprehensive design studies. Each design study is based on characteristics and objectives common to a given profile of network operators having deployed MPLS and discusses all the corresponding design aspects. The book starts with a technology refresher for each of the technologies involved in the design studies. Next, a series of design studies is presented, each based on a specific hypothetical network representative of service provider and enterprise networks running MPLS. Each design study chapter delivers four elements. They open with a description of the network environment, including the set of supported services, the network topology, the POP structure, the transmission facilities, the basic IP routing design, and possible constraints. Then the chapters present design objectives, such as optimizing bandwidth usage. Following these are details of all aspects of the network design, covering VPN, QoS, TE, network recovery, and—where applicable—multicast, IPv6, and pseudowire. The chapters conclude with a summary of the lessons that can be drawn from the design study so that all types of service providers and large enterprise MPLS architects can adapt aspects of the design solution to their unique network environment and objectives. Although network architects have many resources for seeking information on the concepts and protocols involved with

MPLS, there is no single resource that illustrates how to design a network that optimizes their benefits for a specific operating environment. The variety of network environments and requirements makes it difficult to provide a one-size-fits-all design recommendation. Definitive MPLS Network Designs fills this void. "This book comes as a boon to professionals who want to understand the power of MPLS and make full use of it." -Parantap Lahiri, Manager, IP Network Infrastructure Engineering, MCI Includes a FREE 45-Day Online Edition This book is part of the Networking Technology Series from Cisco Press®, which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers.

A complete guide to understanding, designing, and deploying Layer 2 VPN technologies and pseudowire emulation applications Evaluate market drivers for Layer 2 VPNs Understand the architectural frame-work and choices for Layer 2 VPNs, including AToM and L2TPv3 Grasp the essentials of Layer 2 LAN and WAN technologies Examine the theoretical and operational details of MPLS and LDP as they pertain to AToM Understand the theoretical and operational details of Layer 2 protocols over L2TPv3 in IP networks Learn about Layer 2 VPN bridged and routed interworking and Layer 2 local switching Understand the operation and application of Virtual Private LAN Services (VPLS) Learn about foundation and advanced AToM and L2TPv3 topics through an extensive collection of case studies The historical disconnect between legacy Layer 2 and Layer 3 VPN solutions has forced service providers to build, operate, and maintain separate infrastructures to accommodate various VPN access technologies. This costly proposition, however, is no longer necessary. As part of its new Unified VPN Suite, Cisco Systems® now offers next-generation Layer 2 VPN services like Layer 2 Tunneling Protocol version 3 (L2TPv3) and Any Transport over MPLS (AToM) that enable service providers to offer Frame Relay, ATM, Ethernet, and leased-line services over a common IP/MPLS core network. By unifying multiple network layers and providing an integrated set of software services and management tools over this infrastructure, the Cisco® Layer 2 VPN solution enables established carriers, IP-oriented ISP/CLECs, and large enterprise customers (LECs) to reach a broader set of potential VPN customers and offer truly global VPNs. Layer 2 VPN Architectures is a comprehensive guide to consolidating network infrastructures and extending VPN services. The book opens by discussing Layer 2 VPN applications utilizing both AToM and L2TPv3 protocols and comparing Layer 3 versus Layer 2 provider-provisioned VPNs. In addition to describing the concepts related to Layer 2 VPNs, this book provides an extensive collection of case studies that show you how these technologies and architectures work. The case studies include both AToM and L2TPv3 and reveal real-world service provider and enterprise design problems and solutions with hands-on configuration examples and implementation details. The case studies include all Layer 2 technologies transported using AToM and L2TPv3 pseudowires, including Ethernet, Ethernet VLAN, HDLC, PPP, Frame Relay, ATM AAL5 and ATM cells, and advanced topics relevant to Layer 2 VPN deployment, such as QoS and scalability.

Router Security Strategies: Securing IP Network Traffic Planes provides a comprehensive approach to understand and implement IP traffic plane separation and protection on IP routers. This book details the distinct traffic planes of IP networks and the advanced techniques necessary to operationally secure them. This includes the data, control, management, and services planes that provide the infrastructure for IP networking. The first section provides a brief overview of the essential components of the Internet Protocol and IP networking. At the end of this section, you will understand the fundamental principles of defense in depth and breadth security as applied to IP traffic planes. Techniques to secure the IP data plane, IP control plane, IP management plane, and IP services plane are covered in detail in the second section. The final section provides case studies from both the enterprise network and the service provider network perspectives. In this way, the individual IP traffic plane security techniques reviewed in the second section of the book are brought together to help you create an integrated, comprehensive defense in depth and breadth security architecture.

"Understanding and securing IP traffic planes are critical to the overall security posture of the IP infrastructure. The techniques detailed in this book provide protection and instrumentation enabling operators to understand and defend against attacks. As the vulnerability economy continues to mature, it is critical for both vendors and network providers to collaboratively deliver these protections to the IP infrastructure." -Russell Smoak, Director, Technical Services, Security Intelligence Engineering, Cisco Gregg Schudel, CCIE® No. 9591, joined Cisco in 2000 as a consulting system engineer supporting the U.S. service provider organization. Gregg focuses on IP core network security architectures and technology for interexchange carriers and web services providers. David J. Smith, CCIE No. 1986, joined Cisco in 1995 and is a consulting system engineer supporting the service provider organization. David focuses on IP core and edge architectures including IP routing, MPLS technologies, QoS, infrastructure security, and network telemetry. Understand the operation of IP networks and routers Learn about the many threat models facing IP networks, Layer 2 Ethernet switching environments, and IPsec and MPLS VPN services Learn how to segment and protect each IP traffic plane by applying defense in depth and breadth principles Use security techniques such as ACLs, rate limiting, IP Options filtering, uRPF, QoS, RTBH, QPPB, and many others to protect the data plane of IP and switched Ethernet networks Secure the IP control plane with rACL, CoPP, GTSM, MD5, BGP and ICMP techniques and Layer 2 switched Ethernet-specific techniques Protect the IP management plane with password management, SNMP, SSH, NTP, AAA, as well as other VPN management, out-of-band management, and remote access management techniques Secure the IP services plane using recoloring, IP fragmentation control, MPLS label control, and other traffic classification and process control techniques 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.

This book constitutes the refereed post-proceedings of the Second International Conference on Theoretical and Mathematical Foundations of Computer Science, ICTMF 2011, held in Singapore in May 2011. The conference was held together with the Second International Conference on High Performance Networking, Computing, and Communication systems, ICHCC 2011, which proceedings are published in CCIS 163. The 84 revised selected papers presented were carefully reviewed and selected for inclusion in the book. The topics covered range from computational science, engineering and technology to digital signal processing, and computational biology to game theory, and other related topics.

End-to-End Network Security

Router Security Strategies

5th International Conference, ICDCIT 2008 New Delhi, India, December 10 - 12, 2008 Proceedings

Building VPNs

Distributed Computing and Internet Technology

Advanced Science and Technology, Advanced Communication and Networking, Information Security and Assurance, Ubiquitous Computing and Multimedia Appli- tions are conferences that attract many academic and industry professionals. The goal of these

co-located conferences is to bring together researchers from academia and industry as well as practitioners to share ideas, problems and solutions relating to the multifaceted aspects of advanced science and technology, advanced communication and networking, information security and assurance, ubiquitous computing and m- timedia applications. This co-located event included the following conferences: AST 2010 (The second International Conference on Advanced Science and Technology), ACN 2010 (The second International Conference on Advanced Communication and Networking), ISA 2010 (The 4th International Conference on Information Security and Assurance) and UCMA 2010 (The 2010 International Conference on Ubiquitous Computing and Multimedia Applications). We would like to express our gratitude to all of the authors of submitted papers and to all attendees, for their contributions and participation. We believe in the need for continuing this undertaking in the future. We acknowledge the great effort of all the Chairs and the members of advisory boards and Program Committees of the above-listed events, who selected 15% of over 1,000 submissions, following a rigorous peer-review process. Special thanks go to SERSC (Science & Engineering Research Support soCiety) for supporting these - located conferences.

Cisco Express Forwarding

Building MPLS-based Broadband Access VPNs

Mpls Vpn Security