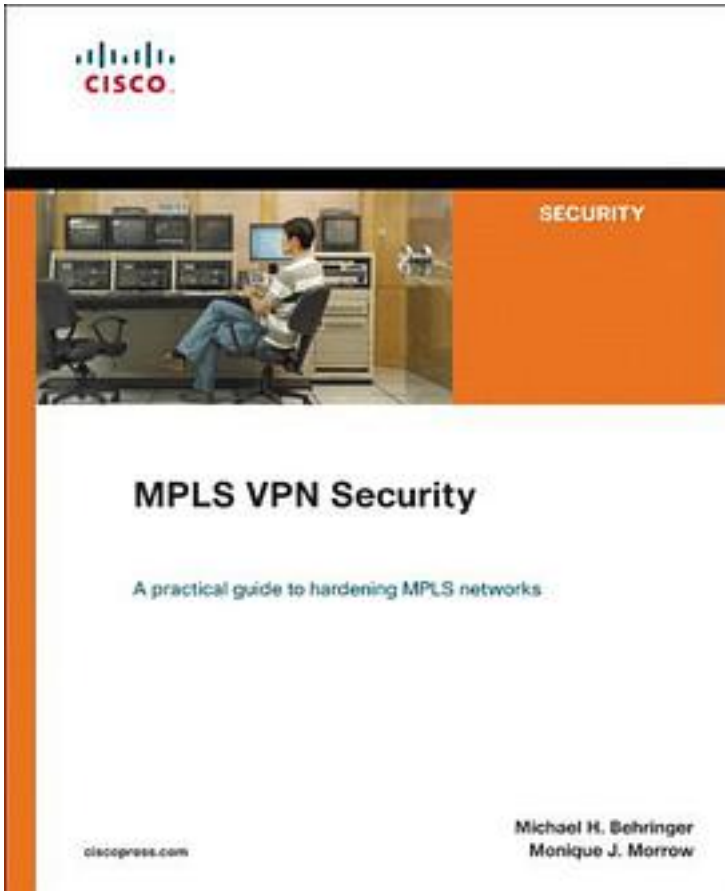
MPLS VPN Security



MPLS VPN Security_下载链接1_

著者:Behringer, Michael H./ Morrow, Monique J.

出版者:Macmillan Technical Pub

出版时间:2005-6

装帧:Pap

isbn:9781587051838

A practical guide to hardening MPLS networks * Define "zones of trust" for your MPLS VPN environment * Understand fundamental security principles and how MPLS VPNs work * Build an MPLS VPN threat model that defines attack points, such as VPN separation, VPN spoofing, DoS against the network's backbone, misconfigurations,

sniffing, and inside attack forms * Identify VPN security requirements, including robustness against attacks, hiding of the core infrastructure, protection against spoofing, and ATM/Frame Relay security comparisons * Interpret complex architectures such as extranet access with recommendations of Inter-AS, carrier-supporting carriers, Layer 2 security considerations, and multiple provider trust model issues * Operate and maintain a secure MPLS core with industry best practices * Integrate IPsec into your MPLS VPN for extra security in encryption and data origin verification * Build VPNs by interconnecting Layer 2 networks with new available architectures such as virtual private wire service (VPWS) and virtual private LAN service (VPLS) * Protect your core network from attack by considering Operations, Administration, and Management (OAM) and MPLS backbone security incidents Multiprotocol Label Switching (MPLS) is becoming a widely deployed technology, specifically for providing virtual private network (VPN) services. Security is a major concern for companies migrating to MPLS VPNs from existing VPN technologies such as ATM. Organizations deploying MPLS VPNs need security best practices for protecting their networks, specifically for the more complex deployment models such as inter-provider networks and Internet provisioning on the network. MPLS VPN Security is the first book to address the security features of MPLS VPN networks and to show you how to harden and securely operate an MPLS network. Divided into four parts, the book begins with an overview of security and VPN technology. A chapter on threats and attack points provides a foundation for the discussion in later chapters. Part II addresses overall security from various perspectives, including architectural, design, and operation components. Part III provides practical guidelines for implementing MPLS VPN security. Part IV presents real-world case studies that encompass details from all the previous chapters to provide examples of overall secure solutions. Drawing upon the authors' considerable experience in attack mitigation and infrastructure security, MPLS VPN Security is your practical guide to understanding how to effectively secure communications in an MPLS environment. "The authors of this book, Michael Behringer and Monique Morrow, have a deep and rich understanding of security issues, such as denial-of-service attack prevention and infrastructure protection from network vulnerabilities. They offer a very practical perspective on the deployment scenarios, thereby demystifying a complex topic. I hope you enjoy their insights into the design of self-defending networks." -Jayshree V. Ullal, Senior VP/GM Security Technology Group, Cisco Systems(R)

作者介绍:

目录:

标签

评论

MPLS VPN Security_下载链接1_

书评

MPLS VPN Security_下载链接1_