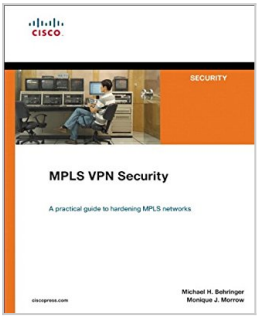

MPLS VPN Security (Self-Study Guide)

By Michael H. Behringer, Monique J. Morrow

MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow

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®

MPLS VPN Security (Self-Study Guide)

By Michael H. Behringer, Monique J. Morrow

MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow

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®

MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow Bibliography

- Sales Rank: #2618207 in eBooks
- Published on: 2005-06-08
- Released on: 2005-06-08
- Format: Kindle eBook

Editorial Review

From the Back Cover
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)

About the Author

Michael H. Behringer is a distinguished engineer at Cisco®, where his expertise focuses on MPLS VPN security, service provider security, and denial-of-service (DoS) attack prevention. Prior to joining Cisco Systems, he was responsible for the design and implementation of pan-European networks for a major European Internet service provider.

Monique J. Morrow is a CTO consulting engineer at Cisco Systems, to which she brings more than 20 years' experience in IP internetworking, design, and service development for service providers. Monique led the engineering project team for one of the first European MPLS VPN deployments for a European Internet service provider.

Users Review

From reader reviews:

Joshua Johnson:

The book MPLS VPN Security (Self-Study Guide) can give more knowledge and information about everything you want. Why then must we leave the good thing like a book MPLS VPN Security (Self-Study Guide)? Several of you have a different opinion about book. But one aim this book can give many facts for us. It is absolutely suitable. Right now, try to closer with your book. Knowledge or information that you take for that, you could give for each other; you could share all of these. Book MPLS VPN Security (Self-Study Guide) has simple shape nevertheless, you know: it has great and massive function for you. You can appearance the enormous world by open and read a book. So it is very wonderful.

David Miller:

The guide with title MPLS VPN Security (Self-Study Guide) has a lot of information that you can understand it. You can get a lot of advantage after read this book. This kind of book exist new understanding the information that exist in this e-book represented the condition of the world right now. That is important to yo7u to find out how the improvement of the world. This book will bring you inside new era of the the positive effect. You can read the e-book in your smart phone, so you can read that anywhere you want.

Alissa Sowell:

People live in this new day of lifestyle always aim to and must have the free time or they will get large amount of stress from both daily life and work. So , once we ask do people have free time, we will say absolutely without a doubt. People is human not a robot. Then we consult again, what kind of activity do you have when the spare time coming to you of course your answer will unlimited right. Then do you try this one, reading publications. It can be your alternative within spending your spare time, the book you have read is definitely MPLS VPN Security (Self-Study Guide).

Kisha Hutton:

Reading a book to become new life style in this season; every people loves to learn a book. When you study a book you can get a large amount of benefit. When you read guides, you can improve your knowledge, due to the fact book has a lot of information onto it. The information that you will get depend on what forms of book that you have read. In order to get information about your research, you can read education books, but if you want to entertain yourself you can read a fiction books, this sort of us novel, comics, along with soon. The MPLS VPN Security (Self-Study Guide) will give you a new experience in examining a book.

Read MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow for online ebook

MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow books to read online.

Online MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow ebook PDF download

MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow Doc

MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow Mobipocket

MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow EPub

SIAY9BDXZ2L: MPLS VPN Security (Self-Study Guide) By Michael H. Behringer, Monique J. Morrow