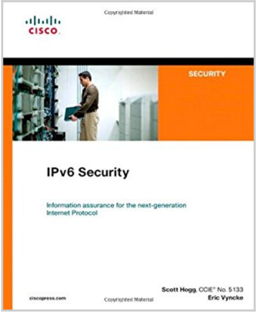

IPv6 Security

By Scott Hogg, Eric Vyncke

IPv6 Security By Scott Hogg, Eric Vyncke

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

IPv6 Security

By Scott Hogg, Eric Vyncke

IPv6 Security By Scott Hogg, Eric Vyncke

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

IPv6 Security By Scott Hogg, Eric Vyncke Bibliography

- Sales Rank: #1462282 in Books
- Brand: Brand: Cisco Press
- Published on: 2008-12-21
- Original language: English
- Number of items: 1
- Dimensions: 9.10" h x 1.40" w x 7.40" l, 2.00 pounds
- Binding: Paperback
- 576 pages

Introduction

Internet Protocol version 6 (IPv6) is the next version of the protocol that is used for communications on the Internet. IPv6 is a protocol that has been in existence for many years, but it has not yet replaced IPv4. IPv4 has some limitations that were not anticipated when it was first created. Because IPv6 overcomes many of these limitations, it is the only viable long-term replacement for IPv4.

While the migration to IPv6 has started, it is still in its early stages. Many international organizations already have IPv6 networks, the U.S. federal organizations are working on their transitions to IPv6, and others are contemplating what IPv6 means to them. However, many organizations already have IPv6 running on their networks and they do not even realize it. Many computer operating systems now default to running both IPv4 and IPv6, which could cause security vulnerabilities if one is less secure than the other. IPv6 security vulnerabilities currently exist, and as the popularity of the IPv6 protocol increases, so do the number of threats.

When a security officer wants to secure an organization, he must be aware of all potential threats, even if this threat is a ten-year-old protocol that represents less than 1 percent of the overall Internet traffic in 2008. Don’t be blinded by this 1 percent: This figure is doomed to increase in the coming years, and chances are good that your network is already exposed to some IPv6 threats. It’s better to be safe than sorry.

Just like the early deployment of many technologies, security is often left to the final stages of implementation. Our intent in writing this book is to improve the security of early IPv6 deployments from day one. Any organization considering or already in the midst of transitioning to IPv6 does not want to deploy a new technology that cannot be secured right from the outset. The transition to IPv6 is inevitable, and therefore this book can help you understand the threats that exist in IPv6 networks and give you ways to protect against them. Therefore, this book gives guidance on how to improve the security of IPv6 networks.

Goals and Methods

Currently, many organizations have slowed their migration to IPv6 because they realize that the security products for IPv6 might be insufficient, despite the fact that the network infrastructure is ready to support IPv6 transport. They realize that they cannot deploy IPv6 without first considering the security of this new protocol. This book intends to survey the threats against IPv6 networks and provide solutions to mitigate those threats. It covers the issues and the best current practices.

This book is arranged so that it covers the threats first and then describes ways to combat these threats. By outlining all the risks and showing that a solution exists for each threat, you can feel more comfortable with continuing the transition to IPv6. You learn about techniques attackers might use to breach your networks and what Cisco products to use to protect the networks.

However, showing attacks without solutions is socially irresponsible, so the focus is on the current techniques that are available to make the IPv6 network more secure and on the best current practices.

By reading this book, you can gain an understanding of the full range of IPv6 security topics.

Who Should Read This Book

This book is intended to be read by people in the IT industry who are responsible for securing computer networks. You should already know the basics of the IPv6 protocol and networking technology. This book is not an introduction to IPv6. There are many good books and online resources that can teach you about IPv6, and there are many great books on computer network security.

The intent of this book is to dive deeper into the protocol and discuss the protocol details from a security practitioner's perspective. It is a book for experts by experts. It covers the theory but at the same time gives practical examples that can be implemented.

How This Book Is Organized

This book starts with a foundation of the security aspects of the IPv6 protocol. The early topics of this book are arranged from the outward perimeter of an organization's network inward to the LAN and server farms. The later chapters of the book cover advanced topics. This book can be read completely from start to finish; however, if you want to "skip around," that is fine. You should eventually read every chapter to gain a comprehensive knowledge of the subject matter.

Some of the information (such as tables and commands) in this book is for reference. You should refer back to this book when it comes time to implement. This gives you cookie-cutter examples to follow that should be in line with the best current practices for securing IPv6. However, do not just go through this book and implement every command listed. Perform some of your own basic research on these commands to make sure that they perform exactly what you intend your network to do.

IPv6 security is an incredibly active research area, and new protocols and new products will continually be developed after this book is written. It is our goal that the "shelf life" of this book is many years because the concepts will still be valid even as Cisco security products continue to evolve with the threat landscape. Every effort was made to make this book as current as possible at the time it was published, but you are advised to check whether new methods are available at the time of reading. The IPv6 security field is quickly evolving as IPv6 gets more widely deployed.

Chapters 1 through 12 cover the following topics:

- **Chapter 1, "Introduction to IPv6 Security":** This short chapter reintroduces IPv6, describes how widely it is deployed, discusses its vulnerabilities, and identifies what hackers already know about IPv6. Some initial mitigation techniques are presented.
- **Chapter 2, "IPv6 Protocol Security Vulnerabilities":** This chapter discusses the aspects of the IPv6 protocol itself that have security implications. Security issues related to ICMPv6 and the IPv6 header structure are covered. Demonstrations are conducted that show the protocol vulnerabilities, and solutions are given to mitigate those risks. This chapter also covers security issues of IPv6 network reconnaissance and address spoofing.
- **Chapter 3, "IPv6 Internet Security":** This chapter covers the large-scale threats against the IPv6 Internet and describes perimeter-filtering techniques that can help protect against those threats. Security for BGP peering is detailed in addition to other service provider–focused security practices. IPv6 MPLS security, security of customer equipment, IPv6 prefix delegation, and multihoming are reviewed.
- **Chapter 4, "IPv6 Perimeter Security":** This chapter covers the security threats that exist for perimeter networks that utilize IPv6. The chapter covers common filtering techniques that are deployed at the perimeter of the network. This chapter also covers IPv6 access lists, the IOS Firewall feature set, and the PIX/ASA/FWSM firewalls.
- **Chapter 5, "Local Network Security":** This chapter examines the threats against LANs. Many vulnerabilities exist on IPv6 access networks, and these vulnerabilities are covered along with many solutions for mitigating them. The chapter covers issues related to Neighbor Discovery Protocol, autoconfiguration addressing, and DHCPv6 communications on a LAN. This chapter also reviews SEND

and describes how it can be implemented.

- **Chapter 6, “Hardening IPv6 Network Devices”:** This chapter covers the security improvements that can be made to a network device running IPv6. Techniques for securing the management of network devices are reviewed. This chapter reviews ways to secure routing protocols and covers first-hop router redundancy protocols. Techniques for controlling the device’s resources are detailed in addition to ways to control network traffic.
- **Chapter 7, “Server and Host Security”:** This chapter covers the ways to secure a computer running IPv6. It is important to harden IPv6 nodes from the threats that exist. Microsoft, Linux, BSD, and Solaris operating system IPv6 security techniques are detailed. This chapter covers how host-based firewalls and Cisco Security Agent (CSA) can be used to protect IPv6 hosts.
- **Chapter 8, “IPsec and SSL Virtual Private Networks”:** This chapter covers the basics of IPsec. The chapter reviews techniques for setting up site-to-site VPN links using IPv6, dynamic multipoint VPNs, as well as remote-access VPNs. The use of ISATAP over an IPsec client connection and the use of SSL VPNs with AnyConnect client are covered.
- **Chapter 9, “Security for IPv6 Mobility”:** This chapter covers Mobile IPv6 and describes how securing this protocol can be challenging. Mobile IPv6 is reviewed, and the security implications are discussed. This chapter gives recommendations on how Mobile IPv6 can be used responsibly and safely. Additional IPv6-capable mobility solutions are covered along with their security implications.
- **Chapter 10, “Securing the Transition Mechanisms”:** This chapter discusses the various techniques that are used to help organizations migrate from IPv4 to IPv6. Dual-stack, tunnel, and NAT migration techniques are covered along with their security issues. Each of these techniques has its own security implications and solutions for securing the traffic. This chapter covers the threats by showing examples of how an attacker might try to infiltrate a network. The security protections that can be used to keep the network safe during migration are also covered.
- **Chapter 11, “Security Monitoring”:** This chapter covers the various systems that are currently available to monitor the security of IPv6 networks. Monitoring a network and the computers on the network is a critical aspect of any security practice. IPv6 networks are the same in this regard and must be managed appropriately. The topics of forensics, intrusion detection and prevention, security information management, and configuration management are covered.
- **Chapter 12, “IPv6 Security Conclusions”:** This chapter summarizes the common themes discussed throughout the book. Commonalities between IPv4 security and IPv6 security are discussed. This chapter contains discussions about creating IPv6-specific security policies. This chapter also reviews what the future holds for IPv6 security. A consolidated list of IPv6 security recommendations is provided.

Read IPv6 Security By Scott Hogg, Eric Vyncke for online ebook

IPv6 Security By Scott Hogg, Eric Vyncke 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 IPv6 Security By Scott Hogg, Eric Vyncke books to read online.

Online IPv6 Security By Scott Hogg, Eric Vyncke ebook PDF download

IPv6 Security By Scott Hogg, Eric Vyncke Doc

IPv6 Security By Scott Hogg, Eric Vyncke Mobipocket

IPv6 Security By Scott Hogg, Eric Vyncke EPub

1CM3YZA6VTD: IPv6 Security By Scott Hogg, Eric Vyncke