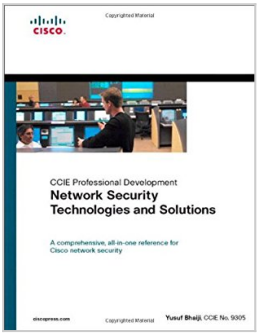

Network Security Technologies and Solutions (CCIE Professional Development Series)

By Yusuf Bhaiji

Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji

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

Network Security Technologies and Solutions (CCIE Professional Development Series)

By Yusuf Bhaiji

Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji

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

Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji Bibliography

- Sales Rank: #1305082 in Books
- Published on: 2008-03-30
- Original language: English
- Number of items: 1
- Dimensions: 9.30" h x 1.93" w x 7.74" l, 3.40 pounds
- Binding: Hardcover
- 840 pages

Introduction

The Internet was born in 1969 as the ARPANET, a project funded by the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. The Internet is a worldwide collection of loosely connected networks that are accessible by individual computers in varied ways, such as gateways, routers, dial-up connections, and through Internet service providers (ISP). Anyone today can reach any device/computer via the Internet without the restriction of geographical boundaries.

As Dr. Vinton G. Cerf states, "The wonderful thing about the Internet is that you're connected to everyone else. The terrible thing about the Internet is that you're connected to everyone else."

The luxury of access to this wealth of information comes with its risks, with anyone on the Internet potentially being the stakeholder. The risks vary from information loss or corruption to information theft and much more. The number of security incidents is also growing dramatically.

With all this happening, a strong drive exists for network security implementations to improve security postures within every organization worldwide. Today's most complex networks require the most comprehensive and integrated security solutions.

Security has evolved over the past few years and is one of the fastest-growing areas in the industry. Information security is on top of the agenda for all organizations. Companies need to keep information secure, and there is an ever-growing demand for the IT professionals who know how to do this.

Point products are no longer sufficient for protecting the information and require system-level security solutions. Linking endpoint and network security is a vital ingredient in designing the modern networks coupled with proactive and adaptive security systems to defend against the new breed of day-zero attacks.

Security is no longer simply an enabling technology or a one-time affair; it has become an essential component of the network blueprint. Security technologies and solutions need to be fundamentally integrated into the infrastructure itself, woven into the fabric of the network. Security today requires comprehensive, end-to-end solutions.

Goals and Methods

Cisco Network Security Technologies and Solutions is a comprehensive all-in-one reference book that covers all major Cisco Security products, technologies, and solutions. This book is a complete reference that helps networking professionals understand and implement current, state-of-the-art security technologies and solutions. The coverage is wide but deep enough to provide the audience with concepts, design, and implementation guidelines as well as basic configuration skills.

With an easy-to-understand approach, this invaluable resource will serve as a central warehouse of security knowledge to the security professionals with end-to-end security implementations.

The book makes no assumption of knowledge level, thereby ensuring that the readers have an explanation that will make sense and be comprehendible at the same time. It takes the reader from the fundamental level of each technology to more detailed descriptions and discussions of each subject.

With this definitive reference, the readers will possess a greater understanding of the solutions available and learn how to build integrated secure networks in today's modern, heterogeneous infrastructure.

This book is comprehensive in scope, including information about mature as well as emerging technologies, including the Adaptive Security Appliance (ASA) Firewall Software Release 8.0, Cisco Intrusion Prevention System (IPS) Sensor Software Release 6.0, Host IPS, Cisco Group Encrypted Transport VPN (GETVPN), MPLS VPN technology, Cisco Distributed Denial-of-Service (DDoS) Anomaly Detection and Mitigation Solutions, Cisco Security Monitoring, Analysis, and Response System (CS-MARS), and Security Framework, Standards and Regulatory Compliance, to name a few.

Who Should Read This Book

Whether you are a network engineer or a security engineer, consultant, or andidate pursuing security certifications, this book will become your primary reference when designing and building a secure network.

Additionally, this book will serve as a valuable resource for candidates preparing for the CCIE Security certification exam that covers topics from the new blueprints.

The book will serve as a reference for any networking professional managing or considering exploring and implementing Cisco network security solutions and technologies.

How This Book Is Organized

This book is meant to complement the information already available on Cisco.com and in the Cisco security products documentation.

The book is divided into five parts, mapping Cisco security technologies and solutions into five key elements.

Part I, "Perimeter Security": This element provides the means to control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Part I includes the following chapters:

- Chapter 1, "Overview of Network Security," introduces principles of network security, security models, and a basic overview of security standards, policies, and the network security framework.
- Chapter 2, "Access Control," describes the capability to perform traffic filtering using access control lists (ACL). It covers numerous types of ACL, such as standard and extended ACL, Lock-and-key, Reflexive, Time-based, Receive ACL, Infrastructure ACL, and Transit ACL. The chapter addresses traffic filtering based on RFC standards and best common practices.
- Chapter 3, "Device Security," covers some of the most common techniques used for device hardening and securing management access for routers, firewall appliances, and the intrusion prevention system (IPS) appliance.
- Chapter 4, "Security Features on Switches," provides a comprehensive set of security features available on the switches. The chapter covers port-level security controls at Layer 2 and security features and best practices available on the switch.
- Chapter 5, "Cisco IOS Firewall," introduces the software-based IOS firewall features, including the legacy Context-Based Access Control (CBAC) and the newly introduced Zone-Based Policy Firewall (ZFW) feature available on the router.
- Chapter 6, "Cisco Firewalls: Appliance and Module," covers the complete range of hardware-based Cisco firewall products, including Cisco PIX, Cisco ASA Firewall appliance, and Cisco Firewall Services Module (FWSM). The chapter provides comprehensive coverage of firewall operating systems (OS), software features, and capabilities.
- Chapter 7, "Attack Vectors and Mitigation Techniques," is a uniquely positioned chapter covering details

of common types of attacks, and providing details of how to characterize and classify various attacks. The chapter provides mitigation techniques for a wide range of attacks at Layer 2 and Layer 3.

Part II, "Identity Security and Access Management": Identity is the accurate and positive identification of network users, hosts, applications, services and resources. Part II includes the following chapters:

- Chapter 8, "Securing Management Access," covers details of the authentication, authorization, and accounting (AAA) framework and implementation of AAA technology. The chapter covers implementing the two widely used security protocols in access management: RADIUS and TACACS+ protocols.
- Chapter 9, "Cisco Secure ACS Software and Appliance," provides details of Cisco Secure Access Control Server (ACS) software that supports the AAA technology and security protocols covered in Chapter 8. The chapter highlights the commonly use ACS software functions and features.
- Chapter 10, "Multifactor Authentication," describes the identification and authentication mechanism using the multifactor authentication system. The chapter introduces common two-factor mechanisms.
- Chapter 11, "Layer 2 Access Control," covers the Cisco trust and identity management solution based on the Identity-Based Networking Services (IBNS) technique. The chapter provides details of implementing port-based authentication and controlling network access at Layer 2 using IEEE 802.1x technology.
- Chapter 12, "Wireless LAN (WLAN) Security," provides an overview of wireless LAN (WLAN) and details of securing WLAN networks. The chapter covers various techniques available to protect WLAN and expands on the various EAP protocols, including EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, and Cisco LEAP. The chapter also provides coverage of common WLAN attacks and mitigation techniques.
- Chapter 13, "Network Admission Control (NAC)" provides details of Cisco Self-Defending Network (SDN) solution using the Cisco Network Admission Control (NAC) appliance-based and framework-based solutions. The chapter covers implementing the Cisco NAC appliance solution as well as the NAC-L3-IP, NAC-L2-IP, and NAC-L2-802.1x solutions.

Part III, "Data Privacy": When information must be protected from eavesdropping, the capability to provide authenticated, confidential communication on demand is crucial. Employing security services at the network layer provides the best of both worlds. VPN solutions can secure communications using confidentiality, integrity, and authentication protocols between devices located anywhere on an untrusted or public network, particularly the Internet. Part III includes the following chapters:

- Chapter 14, "Cryptography," lays the foundation of data privacy and how to secure communication using crypto methodology and cryptographic solutions. The chapter gives a basic overview of various cryptographic algorithms, including hash algorithms, symmetric key, and asymmetric key algorithms.
- Chapter 15, "IPsec VPN," is a comprehensive chapter covering a wide range of IPsec VPN solutions. The chapter provides various types of VPN deployment with focus on IPsec VPN technology covering IPsec protocols, standards, IKE, ISAKMP, and IPsec profiles. The chapter provides comprehensive coverage of implementing IPsec VPN solutions using various methods.
- Chapter 16, "Dynamic Multipoint VPN (DMVPN)," covers the dynamic multipoint VPN (DMVPN) solution architecture and describes the design, components, and how DMVPN works. The chapter provides coverage of implementing various types of DMVPN hub-and-spoke and spoke-to-spoke solutions.
- Chapter 17, "Group Encrypted Transport VPN (GET VPN)," covers the innovative tunnel-less VPN approach to provide data security. The chapter describes the newly introduced GET VPN technology, solution architecture, components, and how GET VPN works.
- Chapter 18, "Secure Sockets Layer VPN (SSL VPN)," describes the SSL-based VPN approach covering SSL VPN solution architecture and various types of SSL VPN. The chapter also covers the newly introduced Cisco AnyConnect VPN.
- Chapter 19, "Multiprotocol Label Switching VPN (MPLS VPN)," provides coverage of Multiprotocol

Label Switching (MPLS)-based VPN technology to provide data security across MPLS networks. The chapter provides MPLS VPN solution architecture and various types of MPLS VPN technologies available. The chapter covers implementing Layer 2 (L2VPN) and Layer 3 (L3VPN)–based MPLS VPN solutions.

Part IV, "Security Monitoring": To ensure that a network remains secure, it's important to regularly test and monitor the state of security preparation. Network vulnerability scanners can proactively identify areas of weakness, and intrusion detection systems can monitor and respond to security events as they occur. Using security monitoring solutions, organizations can obtain unprecedented visibility into both the network data stream and the security posture of the network. Part IV includes the following chapters:

- Chapter 20, "Network Intrusion Prevention," covers network security monitoring using the network-based appliance sensor technology, Intrusion Prevention System (IPS). The chapter provides a comprehensive coverage of the sensor operating system (OS) software functions and features.
- Chapter 21, "Host Intrusion Prevention," covers network security monitoring using the host-based technology, Host Intrusion Prevention System (HIPS). The chapter provides comprehensive details of Cisco Security Agent (CSA) technology providing solution architecture, components, and CSA deployment using CSA MC.
- Chapter 22, "Anomaly Detection," provides coverage of anomaly-based security monitoring using Cisco Anomaly Detection and Mitigation Systems. The chapter covers Cisco Traffic Anomaly Detector and Cisco Guard products to provide DDoS mitigation.
- Chapter 23, "Security Monitoring and Correlation," covers the innovative Security Monitoring, Analysis, and Response System (CS-MARS) based on the Security Threat Mitigation (STM) System. The chapter provides key concepts of CS-MARS and deployment guidelines.

Part V, "Security Management": As networks grow in size and complexity, the requirement for centralized policy management tools grow as well. Sophisticated tools that can analyze, interpret, configure, and monitor the state of security policy, with browser-based user interfaces, enhance the usability and effectiveness of network security solutions. Part V includes the following chapters:

- Chapter 24, "Security and Policy Management," provides comprehensive coverage of the security management solutions using the Cisco Security Manager (CSM) software and various device manager *x*DM tools including SDM, ASDM, PDM, and IDM.
- Chapter 25, "Security Framework and Regulatory Compliance," provides an overview of security standards, policy and regulatory compliance, and best practices frameworks. The chapter covers the two commonly used security frameworks: ISO/IEC 17799 and COBIT. The chapter covers regulatory compliance and legislative acts including GLBA, HIPAA, and SOX.

Network Security Technologies and Solutions is a complete reference book, like a security dictionary, an encyclopedia, and an administrator's guide—all in one.

Read Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji for online ebook

Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji 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 Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji books to read online.

Online Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji ebook PDF download

Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji Doc

Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji Mobipocket

Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji EPub