

## Virtual Private Networks For Beginners Vpn

This introductory guide focuses on networking fundamentals, including design and configuration, hardware, networking protocols, network clients, and security issues.

The TCP/IP protocol suite has become the de facto standard for computer communications in today's networked world. The ubiquitous implementation of a specific networking standard has led to an incredible dependence on the applications enabled by it. Today, we use the TCP/IP protocols and the Internet not only for entertainment and information, but to conduct our business by performing transactions, buying and selling products, and delivering services to customers. We are continually extending the set of applications that leverage TCP/IP, thereby driving the need for further infrastructure support. It is our hope that both the novice and the expert will find useful information in this publication.

What is IPSec? What's a VPN? Why do they need each other? Virtual Private Network (VPN) has become one of the most recognized terms in our industry, yet there continuously seems to be different impressions of what VPNs really are and can become. A Technical Guide to IPSec Virtual Private Networks provides a single point of information that represents hundreds of resources and years of experience with IPSec VPN solutions. It cuts through the complexity surrounding IPSec and the idiosyncrasies of design, implementation, operations, and security. Starting with a primer on the IP protocol suite, the book travels layer by layer through the protocols and the technologies that make VPNs possible. It includes security theory, cryptography, RAS, authentication, IKE, IPSec, encapsulation, keys, and policies. After explaining the technologies and their interrelationships, the book provides sections on implementation and product evaluation. A Technical Guide to IPSec Virtual Private Networks arms information security, network, and system engineers and administrators with the knowledge and the methodologies to design and deploy VPNs in the real world for real companies.

This book tells you how to plan and build a virtual private network, a collection of technologies that creates secure connections or "tunnels" over regular Internet lines. It starts with general concerns like costs and configuration and continues with detailed descriptions of how to install and use useful technologies that are available for Windows NT and UNIX, such as PPTP, the Altavista Tunnel, and the Cisco PIX Firewall.

This new edition gives readers the ability and understanding necessary to create and administer a network. The book shows the reader how to physically connect computers and other devices to a network and access peripherals such as printers over the network.

Learn the basics of optical networking using this practical and easy-to-follow introductory guide. You'll get an overview of concepts behind the technology, as well as helpful information on Cisco, Nortel, and Juniper certifications. Also, a handy 16-page blueprint section offers additional visual instruction.

Virtual Private Networks For Dummies

For Dummies & 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 guide for every VPN management site

"Dennis Fowler provides an insightful view to both the business benefits and technical requirements to VPNs. His examples of other customers' experiences with VPNs breathe life into the discussion." From the Foreword by Susan Scheer Aoko, Cisco systems, Inc. Network-dependent companies are excited by the benefits promised by the virtual private network, including lower costs, greater flexibility, and improvements in connectivity. But they also have questions: What benefits are real? How can they be measured? What are the expenses and the dangers? Virtual Private Networks: Making the Right Connection is an intelligent introduction written especially for business and IT professionals who want a realistic assessment of what a VPN can provide for their organizations. Covering advantages and risks, this book expands your understanding of what you can do with a VPN, while detailing all that implementing it will demand of you. With its help, you'll find your way through VPN hype to the answers you need to make sound decisions. Features Thoroughly explains VPN concepts and technologies, and examines the potential of VPNs as intranets, extranets, and remote access solutions. Covers essential VPN topics like tunneling, encapsulation, encryption, security, and protocols. Provides detailed points of comparison between typical VPN costs and the costs of maintaining traditional WANs. Offers frank consideration of the hidden costs and risks sometimes associated with VPNs, helping you decide if a VPN is right for you. Lists and assesses the software and hardware products you may need to implement a VPN. Discusses both Internet-based VPNs and VPN services offered by providers of "private" ATM and frame relay networks, detailing the pros and cons of each. Data leaks expose your customers to identity theft and your business to security risks. But how do you set up a data loss prevention plan? Start with Data Leaks For Dummies! Now more than ever, it's critical to keep your company data locked up tighter than Fort Knox. Data Leaks For Dummies has the scoop on what's at risk, how leaks happen, how to keep your data safe without being inflexible, and even what to do if the worst happens. It shows you how to: Identify risk by learning to see your data the way a criminal would Recognize how innocent mistakes, common carelessness, and malicious insiders also pose a threat Learn how to defend against phishing, e-mail threats, and wireless security breaches Be alert for social engineering attacks, suspicious contract workers, dumpster divers, and plain old eavesdroppers Plan for safe disposal of old hardware, use caution with SMS and e-mail archives, and be aware of how Webcasts and conference calls can be invaded Discover how crooks steal data in public places such as Internet cafes Develop a recovery plan, build a team, and even manage press coverage should data loss occur You'll learn why free data storage devices could cost you a lot, how to protect mobile devices, why data corruption might be even worse than data loss, and how you can help software developers build safer applications. Data Leaks For Dummies will help you protect your customers, the reputation of your business, and your bottom line.

"Demystifying VPN" is intended to help those individuals with little or no knowledge of internetworking understand VPNs and how they fit into the overall networking environment that includes TCP/IP. The material is presented in a logical fashion, beginning with the basic business reasons for selecting VPNs as a communications solution to the fundamentals of networking and the complexities of VPNs. The material also focuses on the Transmission Control Protocol and Internet Protocol that form the software platform on which VPNs are based, and the Point-to-Point Tunneling Protocol, which is the network protocol supporting VPNs. Michael Busby is an electrical engineer and technical writer in Plano, Texas. He is a consultant; the president of Global Network Services, an international telecommunications company; and the author of "Demystifying ATM/ADSL" and "Demystifying TCP/IP

(3e)".

Are you worried about external hackers and rogue insiders breaking into your systems? Whether it's social engineering, network infrastructure attacks, or application hacking, security breaches in your systems can devastate your business or personal life. In order to counter these cyber bad guys, you must become a hacker yourself—an ethical hacker. Hacking for Dummies shows you just how vulnerable your systems are to attackers. It shows you how to find your weak spots and perform penetration and other security tests. With the information found in this handy, straightforward book, you will be able to develop a plan to keep your information safe and sound. You'll discover how to: Work ethically, respect privacy, and save your system from crashing Develop a hacking plan Treat social engineers and preserve their honesty Counter war dialing and scan infrastructures Understand the vulnerabilities of Windows, Linux, and Novell NetWare Prevent breaches in messaging systems, web applications, and databases Report your results and managing security changes Avoid deadly mistakes Get management involved with defending your systems As we enter into the digital era, protecting your systems and your company has never been more important. Don't let skepticism delay your decisions and put your security at risk. With Hacking For Dummies, you can strengthen your defenses and prevent attacks from every angle!

Worldwide telecom spending was over \$4 trillion in 2004, and virtually all 12 million businesses in the U.S. buy phone and other telecom services Our book shows people at small and medium-sized businesses how to make sense of telecom lingo and get the best deals Includes an overview of the major players in the telecom industry and an easy-to-understand explanation of the existing telecom infrastructure Helps people pinpoint the telecom services best suited to their business needs, understand billing, and troubleshoot problems Covers emerging industry trends, such as Voice over Internet Protocol (VoIP), and how they can help businesses cut costs

Für weltweit tätige Unternehmen gewinnt die Übertragung von Daten, Sprache und Video über virtuelle private Netzwerke (VPN) an Bedeutung. Die Einrichtung von einem Virtuellen Privaten Netzwerk (VPN) ermöglicht es den Nutzern über jede Telefondose oder jedes Wireless LAN auf ihren Arbeitsplatz zuzugreifen über eine sichere Verbindung. Über VPN können sichere und kostengünstige unternehmensweite Netzwerke aufgebaut werden, die sich das öffentliche Netz (Internet) zu Nutze machen. Die Einrichtung eines VPN ist problemlos und inzwischen insbesondere auch für kleinere und mittelgroße Unternehmen erschwinglich. Explains how to create a secure business network over the Internet, link remote sites, and select appropriate hardware and software

Diplomarbeit aus dem Jahr 2003 im Fachbereich Informatik - Internet, neue Technologien, Note: 1,3, Fachhochschule Dortmund (Fachbereich Informatik), Sprache: Deutsch, Abstract: Unternehmungen, die verteilt über verschiedene Standorte evtl. sogar bundesweit oder international arbeiten, müssen mit immensen laufenden Kosten für die benötigten Kommunikationsverbindungen rechnen. Alternativ können durch komplizierte Replikationsverfahren die Daten zu günstigen Zeiten abgeglichen werden, wodurch diese den Anwendungssystemen nicht zeitnah zur Verfügung stehen. Heutige Unternehmen erreichen ihren Erfolg gegenüber dem Wettbewerb zu einem nicht unbeachtlichen Teil dadurch, dass sie Informationen schneller verfügbar haben als der Wettbewerb. Neue preisgünstige Kommunikationslösungen für Unternehmen bergen daher ein beachtliches monatliches Einsparungspotential. So werden durch sog. Internet Service Provider (ISP), Standleitungen ins Internet mit verschiedenen Anschlusstechniken und Bitraten zu günstigen Preisen angeboten. Für die technische Realisierung sollen sog. VPN verwendet werden. Ein Unternehmen das Internetverbindungen als kostengünstige Lösung benutzen möchte, muss die daraus entstehenden Gefährdungen beachten und in die Kalkulation mit einbeziehen. Die bisher von einem Anwender bei einem Kommunikationsanbieter gebräuchlichen Merkmale bzgl. der Qualität, Sicherheit und der Verfügbarkeit sind durch einen ISP meist nicht zu garantieren, da ein ISP nur eingeschränkte Möglichkeiten hat, ausserhalb seines eigenen Internet-Teils auf die oben genannten Merkmale Einfluss zu nehmen. Schon deshalb muss ein Unternehmen, das VPN's betreiben möchte, den sog. Service Level Agreement (SLA)'s der ISP besondere Aufmerksamkeit widmen, und auch mögliche Ausfallszenarien in seinen Betrachtungen mit einfließen lassen. Ob der Einsatz von VPN für Unternehmen aus dem Bereich SOHO sicher und günstig gestaltet werden kann, soll in dieser Diplomarbeit exemplarisch an einem Beispiel ermittelt

An introduction to designing and configuring Cisco IPsec VPNs Understand the basics of the IPsec protocol and learn implementation best practices Study up-to-date IPsec design, incorporating current Cisco innovations in the security and VPN marketplace Learn how to avoid common pitfalls related to IPsec deployment Reinforce theory with case studies, configuration examples showing how IPsec maps to real-world solutions IPsec Virtual Private Network Fundamentals provides a basic working knowledge of IPsec on various Cisco routing and switching platforms. It provides the foundation necessary to understand the different components of Cisco IPsec implementation and how it can be successfully implemented in a variety of network topologies and markets (service provider, enterprise, financial, government). This book views IPsec as an emerging requirement in most major vertical markets, explaining the need for increased information authentication, confidentiality, and non-repudiation for secure transmission of confidential data. The book is written using a layered approach, starting with basic explanations of why IPsec was developed and the types of organizations relying on IPsec to secure data transmissions. It then outlines the basic IPsec/ISAKMP fundamentals that were developed to meet demand for secure data transmission. The book covers the design and implementation of IPsec VPN architectures using an array of Cisco products, starting with basic concepts and proceeding to more advanced topics including high availability solutions and public key infrastructure (PKI). Sample topology diagrams and configuration examples are provided in each chapter to reinforce the fundamentals expressed in text and to assist readers in translating concepts into practical deployment scenarios. Additionally, comprehensive case studies are incorporated throughout to map topics to real-world solutions.

The fast and easy way to get up and running with Windows 10 at work If you want to spend less time figuring out Windows and more time getting things accomplished, you've come to the right place. Covering Windows 10 and packed with time-saving tips to help you get the most out of the software, Windows 10 At Work For Dummies offers everything you need to get back precious hours of your work day and make Windows work for you, rather than against you. This full-color, all-encompassing guide breaks down the most common Windows tasks into easily digestible parts, providing you with illustrated, step-by-step instructions on everything you'll encounter in Windows 10. From setting up your desktop with your favorite apps to finding the files and applications you need and everything in between this hands-on, friendly guide takes the headache out of working with Windows. Provides over 300 tasks broken into core steps Provides easy-to-follow answers to all of your Windows questions Illustrates the new features of Windows 10 If you're a time-pressed professional looking to find answers to all of your Windows-related questions, this is the one-stop resource you'll turn to again and again.

Studienarbeit aus dem Jahr 2020 im Fachbereich Ingenieurwissenschaften - Computertechnik, Note: 2,0, Hochschule Albstadt-Sigmaringen; Albstadt, Sprache: Deutsch, Abstract: Im Rahmen dieser Arbeit soll das Themenfeld VPN - kurz für Virtual Private Network - detaillierter und aus unterschiedlichen Perspektiven beleuchtet werden. So soll im theoretischen Teil neben technischen Grundlagen und verschiedenen Varianten solcher Netzwerke auch auf deren Sicherheit und Nachweismöglichkeiten eingegangen werden. Bevor die Ausarbeitung mit einem

Schlusswort endet, wird im praktischen Teil ein VPN-Server erstellt, mit dem sich ein Client-PC verbindet, wodurch in der Folge der entsprechende Netzwerkverkehr nachgewiesen und analysiert werden soll. Ein Instrument, das während der Corona-Krise zu Beginn des Jahres 2020 immer mehr an Popularität und Bedarf gewann, war Home-Office oder Telearbeit. Dadurch konnten Unternehmen ihren Betrieb weiter aufrechterhalten, ohne ihre Mitarbeiter durch Kontakt im Büro einer erhöhten Infektionsgefahr auszusetzen - zumal der Zuspruch zu Online-Bestellungen, sei es bei Warenhäusern oder Restaurants, auch immer mehr anstieg. Der Kreativität waren dabei kaum Grenzen gesetzt, sei dies bei Home-Office in Form von Erhalt der Arbeit per Post und Mail oder auch bei der Einrichtung von Fernzugriffen und Cloudlösungen auf das Firmennetzwerk. Eine bedeutende Rolle spielten hier auch die VPN(-Netzwerke). Solche Netzwerke waren Teilen der Bevölkerung zwar zumindest in Grundzügen bekannt, jedoch fanden sie bisher vorwiegend Anwendung im informationstechnischen Bereich und wurden weniger für die Arbeit von zuhause aus eingesetzt.

This book provides network managers, LAN administrators and small business operators with all they need to know to "interconnect" multiple locations or travelling employees that need to access a single location. The operation and utilization of virtual private networks is discussed both in theory and practicality, covering the technical aspects associated with encryption and digital certificates as well as the manner by which readers can create VPNs using readily available products from Microsoft, Cisco, Checkpoint and possibly other vendors. The author was among the first to write about the concept of virtual private networking in a series of articles published over five years ago, and in the intervening years this has become a very hot topic - with the technology being increasingly deployed by companies. Virtual Private Networking, by Gilbert Held, covers the technology and the theory, but also shows readers, through numerous examples, 'how to use ' the technology. Step by step guide to connecting all your electronic devices into one network A home network allows you to share Internet connections, photos, video, music, game consoles, printers, and other electronic gadgets. This do-it-yourself guide shows you step by step how to create a wired or wireless network in your home. In the For Dummies tradition of making technology less intimidating, Home Networking Do-It-Yourself For Dummies breaks down the process into easy steps with clear instructions. Increasing broadband speeds, cellular technology, the explosive growth of iPhone sales, and the new Home Group feature in Windows 7 all contribute to a booming interest in home networking This step-by-step guide walks do-it-yourselfers through the process of setting up a wired or wireless network with Windows 7 and Windows Vista Demonstrates how to connect desktops or laptops, printers, a home server, a router, high-speed Internet access, a video game system, a telephone line, and entertainment peripherals Shows how to share files, music, and video, and connect to an iPhone Provides maintenance and troubleshooting tips Home Networking Do-It-Yourself For Dummies enables you to take advantage of everything a home network can offer without hiring a technology wizard.

What's a Gigabook? A collection of just about everything you need to know on a topic, all in one convenient place! Windows XP Gigabook For Dummies takes the best from five other For Dummies books and squeezes out everything but the most important stuff. This single super-sized reference —more than 800 pages' worth — gives you a go-to guide on everything connected with Windows XP, PCs and peripherals, the Internet, Office 2003, and Money 2004. You might think of it as a "greatest hits" collection. Want to know how to set up, navigate, use, and maintain Windows XP? It's all in Book I. Book II covers the care and feeding of PCs in general and takes you on a complete tour of peripherals—those add-ons that make computing cool. Want to explore the world via the World Wide Web? Check Book III. And if you finally have to do some work, check into Book IV, where you'll get the complete story on Office 2003 and Money 2004. You'll discover how to: Customize Windows XP, set up user accounts, and share files Work with digital photos, Windows Media Player, and Windows Movie Maker Choose a printer, scanner, game hardware, and additional storage Set up a wireless home network Get online safely, protect your kids, create your own Webpages, and cruise for bargains on eBay Use Word, Outlook, Excel, and PowerPoint Manage your finances with Microsoft Money Windows XP Gigabook For Dummies is packed with information that's easy to find and even easier to understand. Keep it handy for reference—you'll be glad to see how useful it is!

Put your phone system on your computer network and see the savings See how to get started with VoIP, how it works, and why it saves you money VoIP is techspeak for "voice over Internet protocol," but it could spell "saving big bucks" for your business! Here's where to get the scoop in plain English. Find out how VoIP can save you money, how voice communication travels online, and how to choose the best way to integrate your phone system with your network at home or at the office. Discover how to: Use VoIP for your business or home phone service Choose the best network type Set up VoIP on a wireless network Understand transports and services Demonstrate VoIP's advantages to management

Inhaltsangabe: Einleitung: Der sicherlich größte Nutzen dieser Technologie liegt in der Möglichkeit, die teuren, gemieteten Standleitungen durch billige, frei verfügbare öffentliche Leitungen zu ersetzen. Da aber auch Standleitungen mehr und mehr von Angriffen betroffen sind, wird in letzter Zeit auch dazu übergegangen VPN Technologie über Frame-Relay Verbindungen anzuwenden. Diese Diplomarbeit gibt eine Einführung in die Technologien, die hinter einem Virtuellen Privaten Netzwerk stecken. Es werden die technischen Grundlagen und die möglichen Topologien eines VPN erläutert, und auch die Gefahrenpotentiale im Internet, und die Möglichkeiten, die ein VPN bietet, diese Gefahren zu bekämpfen. Weiters enthält die Arbeit einen Überblick über die in VPNs verwendeten Standards und Protokolle. Es werden dabei die Themen Kryptographie (Verschlüsselung und Authentifikation), Firewalling und die in VPNs verwendeten Protokolle besprochen. Das Hauptaugenmerk liegt in einem Überblick der derzeit am Markt befindlichen VPN-Produkte, kategorisiert nach hardware- und softwarebasierten Produkten, und Firewalls, Switches und Router, die VPN Funktionalitäten implementiert haben. Zu diesen Produkten werden kurze Beschreibungen und die Schlüsselfunktionalitäten des jeweiligen Produktes angeführt. Den Abschluss dieses Kapitels bildet eine Zusammenfassung der beschriebenen Produkte in tabellarischer Form, wo die wichtigsten Funktionalitäten bezüglich VPN dargestellt werden. Inhaltsverzeichnis: Inhaltsverzeichnis: 1. EINFÜHRUNG 9 1.1 Definition von Virtual Private Networking 9 1.2 Vorteile des Einsatzes von VPNs 11 1.3 Mögliche Topologien eines VPN 12 1.3.1 End-To-End-VPN 12 1.3.2 Site-To-Site-VPN 13 1.3.3 End-To-Site-VPN 15 1.4 Die Gefahren im Internet 16 1.4.1 Kryptographische Angriffe 16 1.4.2 Angriffe im Netz 17 1.4.3 Auswirkungen von Angriffen 18 1.4.4 Schutz durch VPN gegen Angriffe 19 2. STANDARDS UND PROTOKOLLE 20 2.1 Kryptographie 20 2.1.1 Einführung 20 2.1.2 Grundlagen 21 2.1.3 Hashalgorithmen 22 2.1.4 Secret-Key-Systeme 22 2.1.5 Public-Key-Systeme 23 2.1.6 Standards 23 2.2 Firewalls 27 2.2.1 Definition 27 2.2.2 Grundlagen 27 2.2.3 Arten von Firewalls 28 2.2.4 Einsatz von Firewalls in einem VPN 30 2.3 Protokolle 31 2.3.1 Grundlagen 31 2.3.2 PAP 35 2.3.3 CHAP 35 2.3.4 MS-CHAP 36 2.3.5 RADIUS 36 2.3.6 SOCKS 37 2.3.7 X.509 38 2.3.8 SSL 39 2.3.9 PPP 40 2.3.10 PPTP 40 2.3.11 L2F 42 2.3.12 L2TP 42 2.3.13 IPSec 43 2.3.14 L2Sec 46 2.3.15 Vergleich IPSec/L2Sec 47 3. MARKTÜBERSICHT VPN 48 3.1 Standalone [...]

Making Everything Easier! Mac OS® X Snow Leopard Server for Dummies Learn to: Set up and configure a Mac network with Snow Leopard Server Administer, secure, and troubleshoot the network Incorporate a Mac subnet into a Windows Active Directory® domain Take advantage of Unix® power and security John Rizzo Want to set up and administer a network even if you don't have an IT department? Read on! Like everything Mac, Snow Leopard Server was designed to be easy to set up and use. Still, there are so many options and features that this book will save you heaps of time and effort. It walks you through installation, set-up on a virtual machine, directory services, managing clients, security, and everything necessary to keep your users happy. Choose your hardware — get all the details on the best hardware for your specific needs It does Windows too — manage Active Directory and Open Directory for a network with both Windows® and Mac® clients Maintain control — create and maintain your User Directory and authenticate clients Files, printers, and stuff — set up user categories and permissions, handle file sharing

protocols, and configure client machines Let's get together — help users collaborate with shared contacts and calendars, Podcast Producer, and iChat® instant messaging The Web world — configure Web services, set up Wiki Server, and enable blogging Out of the office — create mobile accounts for notebook users and configure VPN access Safety first — manage security with firewalls, encryption, and proxies Open the book and find: Various options for installation The pros and cons of Dual Boot How to set up and run an e-mail server Tips on getting Macs and Windows to share files How group accounts can simplify management The advantages of different permission types How to manage Podcast Producer Special stuff in Snow Leopard Server The tools you need to follow your dream of starting and running an online business! With the right knowledge and resources, you can take action to start the online business you've been dreaming of. This comprehensive guide provides tips and tricks for turning your dream into a reality. The sixth edition of *Starting an Online Business: All-in-One For Dummies* will teach you the basics and beyond. It will prepare you to set up your business website, offer your products in an online store, and keep accurate books. The authors help you navigate the primary legal, accounting, and security challenges related to running an online business. Fund your business for success and future growth Use SEO strategically to drive traffic to a well-designed site Market your business effectively as an entrepreneur Stand out, build customer relationships, and sell on social media Keep up with ecommerce trends to stay a step ahead With some guidance, you can find your market niche, create a business plan, and decide on a revenue model. Then, it's time to set up shop! *Starting an Online Business* can help bring your dream of an online business to life and guide you on the road to success.

Choose the best cloud solutions for your needs Cloud computing is a topic that technology pros need to know to stay ahead of the computing game. *Cloud Computing For Dummies* comes to the rescue of those still trying to sort out the many options in the world of cloud. Judith Hurwitz and her team of analysts share the cloud insights they earned by consulting with some of the world's largest companies. Peek inside to sort out topics like multi-cloud architecture, hybrid-cloud infrastructure, development in the cloud, and software as a service. Understand how the cloud can improve your business Explore cloud models including hybrid and multi-cloud environments See how infrastructure and software can be delivered as a service Discover best practices This edition is written for IT professionals, decision makers, and others who need general knowledge about cloud computing, how it works, and what options they have.

The theory, implementation, guidelines, and security aspects of VPNs are covered in this comprehensive book, billed as the only documented resource to protect against common hacker attacks on networks. Written for the Unix, Windows, and NT platforms, this guide provides handy resources and charts to evaluate data trends and perform a cost-benefit analysis.

The authors meet the growing demands of de-centralized companies that need a secure and functional network using Linux. The only book available that extensively covers the combination of VPN technology and Linux, this volume teaches first hand how to build various VPN solutions with individual setup guides.

Secure your CISSP certification! If you're a security professional seeking your CISSP certification, this book is a perfect way to prepare for the exam. Covering in detail all eight domains, the expert advice inside gives you the key information you'll need to pass the exam. Plus, you'll get tips on setting up a 60-day study plan, tips for exam day, and access to an online test bank of questions. *CISSP For Dummies* is fully updated and reorganized to reflect upcoming changes (ISC)<sup>2</sup> has made to the Common Body of Knowledge. Complete with access to an online test bank this book is the secret weapon you need to pass the exam and gain certification. Get key information for all eight exam domains Find test-taking and exam-day tips and tricks Benefit from access to free online practice questions and flash cards Prepare for the CISSP certification in 2018 and beyond You've put in the time as a security professional—and now you can reach your long-term goal of CISSP certification.

A systematic guide to the technologies, standards, protocols, and means used for the transparent security of information interaction in computer networks, this resource enables an independent understanding of the various methods of providing computer and information security when using modern network technology. The basic features of both Web technologies and the distributed information processing technologies connected with them that are based on mobile programs are described, as are the network technologies that influence security. Also covered are the methods of attacking computer networks and practical guidelines for protecting a virtual network.

With the recent availability of high-speed Internet connections to the home and the continued move of workers out of central office locations (whether for travel, telecommuting, or branch office expansion), Virtual Private Networks (VPNs) have become a critical part of corporate network architectures. VPNs use advanced encryption and tunneling to permit your organization to establish secure, end-to-end, private network connections over third-party networks, such as the Internet. This new networking paradigm not only adds to the efficiency of the corporate workforce, but it also saves money by leveraging third-party networks and allows you to scale your networks with greater ease. Based on the official instructor-led training course of the same name, *Cisco Secure Virtual Private Networks* is a comprehensive, results-oriented book designed to give you the knowledge you need to plan, deploy, and manage VPNs in your network environment. Beginning with an overview of VPNs and IPsec, the book introduces you to the Cisco VPN family of products. It then delves into the details of configuring and troubleshooting IPsec site-to-site VPNs on Cisco IOS(r) routers and Cisco PIX(r) Firewalls using preshared keys and digital certificates. You learn how to install the VPN 3000 Concentrator and how to configure it for remote access using preshared keys and digital certificates. Monitoring and administration techniques are also presented. The book concludes with a discussion on the scalability solutions available for IPsec VPNs. Each chapter includes an explicit set of learning objectives and concludes with a set of review questions to assess your understanding of the material. Numerous examples are provided throughout, and detailed diagrams help clarify concepts presented in the text. Whether you are preparing for the Cisco Security Specialist 1 certification or simply want to understand and make the most efficient use of VPNs, *Cisco Secure Virtual Private Networks* provides you with a complete solution for designing, implementing, and managing Cisco VPN networks. Prepare for the Cisco Security Specialist 1 VPN exam with the official CSVPN Coursebook Evaluate the features, functions, and benefits of Cisco VPN products Understand the component technologies that are implemented in Cisco VPN products Learn the procedures, steps, and commands required to configure and test IPsec in Cisco IOS Software and the Cisco PIX Firewall Install and configure the Cisco VPN client to create a secure tunnel to a Cisco VPN Concentrator and Cisco PIX Firewall Configure and verify IPsec in the Cisco VPN Concentrator, Cisco router, and Cisco PIX Firewall Enable interoperability among the Cisco VPN Concentrator, Cisco routers, and Cisco PIX Firewalls Apply scalability and advanced configuration features supported in the Cisco IPsec implementation Andrew G. Mason, CCIE(r) #7144, CSS-1, CCNP(r): Security, and CCDP(r), is the CEO of three UK-based companies: Mason Technologies, CCStudy.com, and Boxing

Orange. Andrew has 11 years experience in the networking industry and is currently consulting for the largest ISP in the UK. He is involved daily in the design and implementation of complex secure hosted solutions utilizing products from the Cisco Secure family.

Becoming a master of networking has never been easier Whether you're in charge of a small network or a large network, Networking All-in-One is full of the information you'll need to set up a network and keep it functioning. Fully updated to capture the latest Windows 10 releases through Spring 2018, this is the comprehensive guide to setting up, managing, and securing a successful network. Inside, nine minibooks cover essential, up-to-date information for networking in systems such as Windows 10 and Linux, as well as best practices for security, mobile and cloud-based networking, and much more. Serves as a single source for the most-often needed network administration information Covers the latest trends in networking Get nine detailed and easy-to-understand networking minibooks in one affordable package Networking All-in-One For Dummies is the perfect beginner's guide as well as the professional's ideal reference book. In the five years since the first edition of this classic book was published, Internet use has exploded. The commercial world has rushed headlong into doing business on the Web, often without integrating sound security technologies and policies into their products and methods. The security risks--and the need to protect both business and personal data--have never been greater. We've updated Building Internet Firewalls to address these newer risks. What kinds of security threats does the Internet pose? Some, like password attacks and the exploiting of known security holes, have been around since the early days of networking. And others, like the distributed denial of service attacks that crippled Yahoo, E-Bay, and other major e-commerce sites in early 2000, are in current headlines. Firewalls, critical components of today's computer networks, effectively protect a system from most Internet security threats. They keep damage on one part of the network--such as eavesdropping, a worm program, or file damage--from spreading to the rest of the network. Without firewalls, network security problems can rage out of control, dragging more and more systems down. Like the bestselling and highly respected first edition, Building Internet Firewalls, 2nd Edition, is a practical and detailed step-by-step guide to designing and installing firewalls and configuring Internet services to work with a firewall. Much expanded to include Linux and Windows coverage, the second edition describes: Firewall technologies: packet filtering, proxying, network address translation, virtual private networks Architectures such as screening routers, dual-homed hosts, screened hosts, screened subnets, perimeter networks, internal firewalls Issues involved in a variety of new Internet services and protocols through a firewall Email and News Web services and scripting languages (e.g., HTTP, Java, JavaScript, ActiveX, RealAudio, RealVideo) File transfer and sharing services such as NFS, Samba Remote access services such as Telnet, the BSD "r" commands, SSH, BackOrifice 2000 Real-time conferencing services such as ICQ and talk Naming and directory services (e.g., DNS, NetBT, the Windows Browser) Authentication and auditing services (e.g., PAM, Kerberos, RADIUS); Administrative services (e.g., syslog, SNMP, SMS, RIP and other routing protocols, and ping and other network diagnostics) Intermediary protocols (e.g., RPC, SMB, CORBA, IIOP) Database protocols (e.g., ODBC, JDBC, and protocols for Oracle, Sybase, and Microsoft SQL Server) The book's complete list of resources includes the location of many publicly available firewall construction tools.

Sie sind ein erfolgreicher Hacker, finden jede Sicherheitslücke, überwinden jede Firewall und sind es gewohnt, immer an Ihr Ziel zu kommen? Dann haben wir jetzt schlechte Nachrichten für Sie: Dieses Buch wird Ihnen das Leben schwer machen! Dem Autor gelingt es, solide und verständlich das Hintergrundwissen über Netzwerk- und Datensicherheit zu vermitteln, das Ihnen das Handwerk legt. Kein Problem - mir fällt immer etwas Neues ein, das nicht im Buch steht, denken Sie? Dann haben wir noch eine schlechte Nachricht: Ihre neuesten Tricks verraten wir immer aktuell auf der Homepage zum Buch. "Fern marktschreierischer Glätte und Oberflächlichkeit sowie akademischer Sperrigkeit und Praxisfeindlichkeit ist Kappes eine solide Einführung gelungen, die mit jeder Seite zeigt, dass der Autor um die Bedürfnisse seiner Leser in Sachen IT-Sicherheit weiß." Buchkatalog.de, 29.05.2008

Wireless home networks are better than ever! The emergence of new industry standards has made them easier, more convenient, less expensive to own and operate. Still, you need to know what to look for (and look out for), and the expert guidance you'll find in Wireless Home Networks For Dummies, 3rd Edition helps you ensure that your wire-free life is also a hassle-free life! This user-friendly, plain-English guide delivers all of the tips, tricks, and knowledge you need to plan your wireless home network, evaluate and select the equipment that will work best for you, install and configure your wireless network, and much more. You'll find out how to share your Internet connection over your network, as well as files, printers, and other peripherals. And, you'll learn how to avoid the "gotchas" that can creep in when you least expect them. Discover how to: Choose the right networking equipment Install and configure your wireless network Integrate Bluetooth into your network Work with servers, gateways, routers, and switches Connect audiovisual equipment to your wireless network Play wireless, multiuser computer games Establish and maintain your network's security Troubleshoot networking problems Improve network performance Understand 802.11n Whether you're working with Windows PCs, Mac OS X machines, or both Wireless Home Networking For Dummies, 3rd Edition, makes it fast and easy to get your wireless network up and running—and keep it that way!

Let's face it: the information age makes dummies of us all at some point. One thing we can say for sure, though, about things related to the Internet is that their best strengths are often also their worst weaknesses. This goes for virtual private networks (VPNs). They may reach a wide base of customers – but can also be vulnerable to viruses, hackers, spoofers, and other shady online characters and entities. VPNs may allow for super-efficient communication between customer and company – but they rely on information which, if compromised, can cause huge losses. The Internet is still a frontier – sometimes so wide open it leaves us bewildered – and, like any frontier, the risks go hand in hand with potentially huge rewards. Virtual Private Networks for Dummies offers you a no-nonsense, practical guide to evaluating your company's need for a VPN, understanding what it takes to implement one, and undertaking the challenging quest to

set it up, make it work, and keep it safe. Whether you're the resident expert leading the project team, or you just want to learn what makes e-commerce tick, this detailed, from-the-ground-up guide will soon have you comfortably conceptualizing: Security goals and strategies The evolution of VPNs Privacy in VPNs Extranets Remote-Access VPNs Funding Custom network solutions design Testing VPNs And more With new products and technologies offering supposedly revolutionary solutions to IT departments every day, this book focuses on the real world – you know, the one full of obstacles, mishaps, threats, delays, and errors – and gives you the background knowledge to make decisions for yourself about your VPN needs. Written with a dash of humor, Virtual Private Networks for Dummies contains both technical detail (standards, protocols, etc.) and more general concepts (such as conducting cost-benefit analyses). This clear, authoritative guide will have you securely and cost-effectively networking over the Internet in no time.

[Copyright: b2283534c47027a0040e6517fe020f44](#)