

## Cisco ASA Firewall Using AAA And ACS - ASA 9 1 (Cisco Pocket Lab Guides Book 3)

Become a Cisco security specialist by developing your skills in network security and explore advanced security technologies Key Features Enhance your skills in network security by learning about Cisco’s device configuration and installation Unlock the practical aspects of CCNA security to secure your devices Explore tips and tricks to help you achieve the CCNA Security 210-260 Certification Book Description With CCNA Security certification, a network professional can demonstrate the skills required to develop security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security 210-260 Certification Guide will help you grasp the fundamentals of network security and prepare you for the Cisco CCNA Security Certification exam. You’ll begin by getting a grip on the fundamentals of network security and exploring the different tools available. Then, you’ll see how to securely manage your network devices by implementing the AAA framework and configuring different management plane protocols. Next, you’ll learn about security on the data link layer by implementing various security toolkits. You’ll be introduced to various firewall technologies and will understand how to configure a zone-based firewall on a Cisco IOS device. You’ll configure a site-to-site VPN on a Cisco device and get familiar with different types of VPNs and configurations. Finally, you’ll delve into the concepts of IPS and endpoint security to secure your organization’s network infrastructure. By the end of this book, you’ll be ready to take the CCNA Security Exam (210-260). What you will learn Grasp the fundamentals of network security Configure routing protocols to secure network devices Mitigate different styles of security attacks using Cisco devices Explore the different types of firewall technologies Discover the Cisco ASA functionality and gain insights into some advanced ASA configurations Implement IPS on a Cisco device and understand the concept of endpoint security Who this book is for CCNA Security 210-260 Certification Guide can help you become a network security engineer, a cyber security professional, or a security administrator. You should have valid CCENT or CCNA Routing and Switching certification before taking your CCNA Security exam. CCIE Security v3.0 Configuration Practice Labs presents you with two full lab scenarios in exam style format to echo the actual eight hour CCIE Security lab exam. This publication gives you the opportunity to put into practice your own extensive theoretical knowledge of the broad range of topics covered on the CCIE Security lab exam to see how they interact with each other on a larger, more complex scale. An “Ask the Proctor” section list of questions for each section helps provide clarity and maintain direction, answering the most common questions candidates ask proctors in the actual exam. After each lab, this eBook lets you compare configurations and routing tables with the required answers. You can also run through a lab de-brief, view configurations, and cut and paste configs into your own lab equipment for testing and verification. The point scoring for each question lets you know if you passed or failed each lab. Developed by the CCIE Security program manager, these comprehensive practice labs that sell for hundreds of dollars elsewhere help make sure you are fully prepared for the grueling CCIE Security lab exam experience.

Automating Cisco Security Solutions (SAUTO 300-735) training course is associated with the CCNP Security Certification and DevNet Professional Certification. It is especially useful for those leading or participating in projects. This course is ideal for: -Network engineer -Systems engineer -Wireless engineer -Consulting systems engineer -Technical solutions architect -Network administrator -Wireless design engineer -Network manager -Sales engineer -Account manager Preparing for Automating Cisco Security Solutions (SAUTO 300-735)? Here we have brought Best Exam Questions for you so that you can prepare well for this Exam of Automating Cisco Security Solutions (SAUTO 300-735). Unlike other online simulation practice tests, you get a eBook version that is easy to read & remember these questions. You can simply rely on these questions for successfully certifying this exam.

The Best Damn Cisco Internetworking Book Period shows readers everything they need to know about all Cisco internetworking topics. The book provides an understanding of Cisco’s current VoIP solutions and the means to put them to work, showing how to configure all of Cisco’s core VoIP products—among them Cisco CallManager software, Cisco 7910 series phones, and server-based IP PBXs. It discusses IPv6 Protocols, as well as IP Quality of Service (QoS) and how it applies to Enterprise and Internet Service Provider (ISP) environments. In addition, Cisco wireless technologies are covered in detail. Cisco has placed a high priority on security and here readers will find complete coverage of all the Cisco Security products such as the PIX firewall suite of products, Network Address Translation (NAT), Cisco VPN Concentrator and IPsec, Cisco Authentication, Authorization, and Accounting (AAA), Content Services Switch (CSS), and the Cisco Secure Network Intrusion Detection System. This book is sure to become a go eared reference for all Cisco engineers and administrators. - The one book that covers all major Cisco Internetworking concepts and configurations. - The only book to cross reference Cisco internetworking topics: Voice Over IP, Remote Access, Wireless, AVVID, and QoS. In addition, new technologies are covered in depth: AVVID, SIP, MGCP, and more. - A 1-stop reference for Cisco professionals needing coverage of core Cisco exam topics.

IBM and Cisco: Together for a World Class Data Center

Cisco ASA Configuration

Cisco Certified CyberOps Associate 200-201 Certification Guide

All-in-one Firewall, IPS, and VPN Adaptive Security Appliance

Cisc ISE BYOD Secu ePub 2

Computer Network Security

Trust the best selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for exam success. They are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. CCNA Security 640-554 Official Cert Guide presents you with an organized test preparation routine through the use of proven series elements and techniques. “Do I Know This Already?” quizzes open each chapter and enable you to decide how much time you need to spend on each section. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. · Master Cisco CCNA Security 640-554 exam topics · Assess your knowledge with chapter-opening quizzes · Review key concepts with exam preparation tasks · Practice with realistic exam questions on the CD-ROM CCNA Security 640-554 Official Cert Guide, focuses specifically on the objectives for the Cisco CCNA Security IINS exam. Expert networking professionals Keith Barker and Scott Morris share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The companion CD-ROM contains a powerful Pearson IT Certification Practice Test engine that enables you to focus on individual topic areas or take complete, timed exams. The assessment engine also tracks your performance and provides feedback on a module-by-module basis, laying out a complete assessment of your knowledge to help you focus your study where it is needed most. The CD also contains 90 minutes of video training on CCP, NAT, object groups, ACLs, port security on a Layer 2 switch, CP3L, and zone-based firewalls. Well-regarded for its level of detail, assessment features, comprehensive design scenarios, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The official study guide helps you master all the topics on the CCNA Security IINS exam, including: Network security concepts Security policies and strategies Network foundation protection (NFP) Cisco Configuration Professional (CCP) Management plane security AAA security Layer 2 security threats IPv6 security Threat mitigation and containment Access Control Lists (ACLs) Network Address Translation (NAT) Cisco IOS zone-based firewalls and ASA firewalls Intrusion prevention and detection systems Public Key Infrastructure (PKI) and cryptography Site-to-site IPsec VPNs and SSL VPNs CCNA Security 640-554 Official Cert Guide is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining. The print edition of the CCNA Security 640-554 Official Cert Guide contains 90 minutes of video instruction, two free, complete practice exams as well as an exclusive offer for 70% off Premium Edition eBook and Practice Test. Pearson IT Certification Practice Test minimum system requirements: Windows XP (SP3), Windows Vista (SP2), or Windows 7; Microsoft .NET Framework 4.0 Client; Pentium class 1GHz processor (or equivalent); 512 MB RAM; 650 MB disc space plus 50 MB for each downloaded practice exam Also available from Cisco Press for Cisco CCNA Security study is the CCNA Security 640-554 Official Cert Guide Premium Edition eBook and Practice Test. This digital-only certification preparation product combines an eBook with enhanced Pearson IT Certification Practice Test. This integrated learning package: · Allows you to focus on individual topic areas or take complete, timed exams · Includes direct links from each question to detailed tutorials to help you understand the concepts behind the questions · Provides unique sets of exam-realistic practice questions · Tracks your performance and provides feedback on a module-by-module basis, laying out a complete assessment of your knowledge to help you focus your study where it is needed most

As a network administrator, auditor or architect, you know the importance of securing your network and finding security solutions you can implement quickly. This succinct book departs from other security literature by focusing exclusively on ways to secure Cisco routers, rather than the entire network. The rational is simple: If the router protecting a network is exposed to hackers, then so is the network behind it. Hardening Cisco Routers is a reference for protecting the protectors. Included are the following topics: The importance of router security and where routers fit into an overall security plan Different router configurations for various versions of Cisco’s IOS Standard ways to access a Cisco router and the security implications of each Password and privilege levels in Cisco routers Authentication, Authorization, and Accounting (AAA) control Router warning banner use (as recommended by the FBI) Unnecessary protocols and services commonly run on Cisco routers SNMP security Anti-spoofing Protocol security for RIP, OSPF, EIGRP, NTP, and BGP Logging violations Incident response Physical security Written by Thomas Akin, an experienced Certified Information Systems Security Professional (CISSP) and Certified Cisco Academic Instructor (CCAI), the book is well organized, emphasizing practicality and a hands-on approach. At the end of each chapter, Akin includes a Checklist that summarizes the hardening techniques discussed in the chapter. The Checklists help you double-check the configurations you have been instructed to make, and serve as quick references for future security procedures.Concise and to the point, Hardening Cisco Routers supplies you with all the tools necessary to turn a potential vulnerability into a strength. In an area that is otherwise poorly documented, this is the one book that will help you make your Cisco routers rock solid.

Covers the most important and common configuration scenarios and features which will put you on track to start implementing ASA firewalls right away.

As a final exam preparation tool, CCNP Security Firewall 642-618 Quick Reference provides a concise review of all objectives on the new CCNP Security Firewall exam (642-618). This eBook provides you with detailed, graphical-based information, highlighting only the key topics in cram-style format. With this document as your guide, you will review topics on firewall basics, the ASA product family, ASA configuration with both the CLI and ASDM, ASA access control, ASA network integration, AAA configuration, and ASA HA. This fact-filled Quick Reference allows you to get all-important information at a glance, helping you to focus your study on areas of weakness and to enhance memory retention of essential exam concepts.

Learn blue teaming strategies and incident response techniques to mitigate cybersecurity incidents

CCIE Security v3.0 Configuration Practice Labs

The Best Damn Cisco Internetworking Book Period

Build your knowledge of network security and pass your CCNA Security exam (210-260)

Hardening Cisco Routers

Cisco IOS Cookbook

Trust the best selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for exam success. They are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. Master Cisco CCNA Security 210-260 Official Cert Guide exam topics –Assess your knowledge with chapter-opening quizzes –Review key concepts with exam preparation tasks This is the eBook edition of the CCNA Security 210-260 Official Cert Guide. This eBook does not include the companion CD-ROM with the practice exam that comes with the print edition. CCNA Security 210-260 Official Cert Guide presents you with an organized test preparation routine through the use of proven series elements and techniques. “Do I Know This Already?” quizzes open each chapter and enable you to decide how much time you need to spend on each section. Exam topics lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. CCNA Security 210-260 Official Cert Guide focuses specifically on the objectives for the Cisco CCNA Security exam. Networking Security experts Omar Santos and John Stuppi share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. Well-regarded for its level of detail, assessment features, comprehensive design scenarios, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The official study guide helps you master all the topics on the CCNA Security exam, including –Networking security concepts –Common security threats –Implementing AAA using IOS and ISE –Bringing Your Own Device (BYOD) –Fundamentals of VPN technology and cryptography –Fundamentals of IP security –Implementing IPsec site-to-site VPNs –Implementing SSL remote-access VPNs using Cisco ASA –Securing Layer 2 technologies –Network Foundation Protection (NFP) –Securing the management plane on Cisco IOS devices –Securing the data plane –Securing routing protocols and the control plane –Understanding firewall fundamentals –Implementing Cisco IOS zone-based firewalls –Configuring basic firewall policies on Cisco ASA –Cisco IOS fundamentals –Mitigation technologies for e-mail- and web-based threats –Mitigation technologies for endpoint threats CCNA Security 210-260 Official Cert Guide is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit http://www.cisco.com/web/learning/index.html.

The real-world guide to securing Cisco-based IP telephony applications, devices, and networks Cisco IP telephony leverages converged networks to dramatically reduce TCO and improve ROI. However, its critical importance to business communications and deep integration with enterprise IP networks make it susceptible to attacks that legacy telecom systems did not face. Now, there’s a comprehensive guide to securing the IP telephony components that ride atop data network infrastructures—and thereby providing IP telephony services that are safer, more resilient, more stable, and more scalable. Securing Cisco IP Telephony Networks provides comprehensive, up-to-date details for securing Cisco IP telephony equipment, underlying infrastructure, and telephony applications. Drawing on ten years of experience, senior network consultant Akhil Behl offers a complete security framework for use in any Cisco IP telephony environment. You’ll find best practices and detailed configuration examples for securing Cisco Unified Communications Manager (CUCM), Cisco Unity/Unity Connection, Cisco Unified Presence, Cisco Voice Gateways, Cisco IP Telephony Endpoints, and many other Cisco IP Telephony applications. The book showcases easy-to-follow Cisco IP Telephony applications and network security-centric examples in every chapter. This guide is invaluable to every technical professional and IT decision-maker concerned with securing Cisco IP telephony networks, including network engineers, administrators, architects, managers, security analysts, IT directors, and consultants. Recognize vulnerabilities caused by IP network integration, as well as VoIP’s unique security requirements Discover how hackers target IP telephony networks and proactively protect against each facet of their attacks Implement a flexible, proven methodology for end-to-end Cisco IP Telephony security Use a layered (defense-in-depth) approach that builds on underlying network security design Secure CUCM, Cisco Unity/Unity Connection, CUPS, CUCM Express, and Cisco Unity Express platforms against internal and external threats Establish physical security, Layer 2 and Layer 3 security, and Cisco ASA-based perimeter security Complete coverage of Cisco IP telephony encryption and authentication fundamentals Configure Cisco IOS Voice Gateways to help prevent toll fraud and deter attacks Secure Cisco Voice Gatekeepers and Cisco Unified Border Element (CUBE) against rogue endpoints and other attack vectors Secure Cisco IP telephony endpoints–Cisco Unified IP Phones (wired, wireless, and soft phone) from malicious insiders and external threats This IP communications book is part of the Cisco Press® Networking Technology Series. IP communications titles from Cisco Press help networking professionals understand voice and IP telephony technologies, plan and design converged networks, and implement network solutions for increased productivity.

Begin a successful career in cybersecurity operations by achieving Cisco Certified CyberOps Associate 200-201 certification Key Features Receive expert guidance on how to kickstart your career in the cybersecurity industryGain hands-on experience while studying for the Cisco Certified CyberOps Associate certification examWork through practical labs and exercises mapped directly to the exam objectives Book Description Achieving the Cisco Certified CyberOps Associate 200-201 certification helps you to kickstart your career in cybersecurity operations. This book offers up-to-date coverage of 200-201 exam resources to help you equip you to pass on your first attempt. The book covers the essentials of network security concepts and shows you how to perform security threat monitoring. You’ll begin by gaining an in-depth understanding of cryptography and exploring the methodology for performing both host and network-based intrusion analysis. Next, you’ll learn about the importance of implementing security management and incident response strategies in an enterprise organization. As you advance, you’ll see why implementing defenses is necessary by taking an in-depth approach, and then perform security monitoring and packet analysis on a network. You’ll also discover the need for computer forensics and get to grips with the components used to identify network intrusions. Finally, the book will not only help you to learn the theory but also enable you to gain much-needed practical experience for the cybersecurity industry. By the end of this Cisco cybersecurity book, you’ll have covered everything you need to pass the Cisco Certified CyberOps Associate 200-201 certification exam, and have a handy, on-the-job desktop reference guide. What you will learn Incorporate security into your architecture to prevent attacksDiscover how to implement and prepare secure designsIdentify access control models for digital assetsIdentify point of entry, determine scope, contain threats, and remediateFind out how to perform malware analysis and interpretationImplement security technologies to detect and analyze threats Who this book is for This book is for students who want to pursue a career in cybersecurity operations, threat detection and analysis, and incident response. IT professionals, network security engineers, security operations center (SOC) engineers, and cybersecurity analysts looking for a career boost and those looking to get certified in Cisco cybersecurity technologies and break into the cybersecurity industry will also benefit from this book. No prior knowledge of IT networking and cybersecurity industries is needed.

Cisco Firewalls Concepts, design and deployment for Cisco Stateful Firewall solutions 2 In this book, Alexandre proposes a totally different approach to the important subject of firewalls: Instead of just presenting configuration models, he uses a set of carefully crafted examples to illustrate the theory in action. A must read! —Luc Billot, Security Consulting Engineer at Cisco 2 Cisco Firewalls thoroughly explains each of the leading Cisco firewall products, features, and solutions, and shows how they can add value to any network security design or operation. The author tightly links theory with practice, demonstrating how to integrate Cisco firewalls into highly secure, self-defending networks. Cisco Firewalls shows you how to deploy Cisco firewalls as an essential component of every network infrastructure. The book takes the unique approach of illustrating complex configuration concepts through step-by-step examples that demonstrate the theory in action. This is the first book with detailed coverage of firewalling Unified Communications systems, network virtualization architectures, and environments that include virtual machines. The author also presents indispensable information about integrating firewalls with other security elements such as IPS, VPNs, and load balancers; as well as a complete introduction to firewalling IPv6 networks. Cisco Firewalls will be an indispensable resource for engineers and architects designing and implementing firewalls; security administrators, operators, and support professionals; and anyone preparing for the CCNA Security, CCNP Security, or CCIE Security certification exams. 2 Alexandre Matos da Silva Pires de Moraes, CCIE No. 8063, has worked as a Systems Engineer for Cisco Brazil since 1998 in projects that involve not only Security and VPN technologies but also Routing Protocol and Campus Design, IP Multicast Routing, and MPLS Networks Design. He coordinated a team of Security engineers in Brazil and holds the CISSP, CCSP, and three CCIE certifications (Routing/Switching, Security, and Service Provider). A frequent speaker at Cisco Live, he holds a degree in electronic engineering from the Instituto Tecnológico de Aeronáutica (ITA – Brazil). 2 2 Create advanced security designs utilizing the entire Cisco firewall product family 2 2 Implement flexible security policies with the Zone Policy Firewall (ZPF) 2 2 Strengthen threat inspection with antispooling, TCP normalization, connection limiting, and IP fragmentation handling 2 2 Inspect IP voice protocols, including SCCP, H.323, SIP, and MGCP 2 2 Utilize identity to provide user-based stateful functionality 2 2 Understand how multicast traffic is handled through firewalls 2 2 Use firewalls to protect your IPv6 deployments 2 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.

CCNA Security 210-260 Official Cert Guide

Cisco Firewalls

Cisco ASA

Cisco ASA for Accidental Administrators

Network Security First-step

Concepts and Tools

Cisco’s complete, authoritative guide to Authentication, Authorization, and Accounting (AAA) solutions with CiscoSecure ACS AAA solutions are very frequently used by customers to provide secure access to devices and networks AAA solutions are difficult and confusing to implement even though they are almost mandatory Helps IT Pros choose the best identity management protocols and designs for their environments Covers AAA on Cisco routers, switches, access points, and firewalls This is the first complete, authoritative, single-source guide to implementing, configuring, and managing Authentication, Authorization and Accounting (AAA) identity management with CiscoSecure Access Control Server (ACS) 4 and 5. Written by three of Cisco’s most experienced CiscoSecure product support experts, it covers all AAA solutions (except NAC) on Cisco routers, switches, access points, firewalls, and concentrators. It also thoroughly addresses both ACS configuration and troubleshooting, including the use of external databases supported by ACS. Each of this book’s six sections focuses on specific Cisco devices and their AAA configuration with ACS. Each chapter covers configuration syntax and examples, debug output with explanations, and ACS screenshots. Drawing on the authors’ experience with several thousand support cases in organizations of all kinds, AAA Identity Management Security pitfalls, warnings, and tips throughout. Each major topic concludes with a practical, hands-on lab scenario corresponding to a real-life solution that has been widely implemented by Cisco customers. This book brings together crucial information that was previously scattered across multiple sources. It will be indispensable to every professional running CiscoSecure ACS 4 or 5, as well as all candidates for CCSP and CCIE (Security or R and S) certification.

This IBM® Redbooks® publication is an IBM and Cisco collaboration that articulates how IBM and Cisco can bring the benefits of their respective companies to the modern data center. It documents the architectures, solutions, and benefits that can be achieved by implementing a data center based on IBM server, storage, and integrated systems, with the broader Cisco network. We describe how to design a state-of-the-art data center and networking infrastructure combining Cisco and IBM solutions. The objective is to provide a reference guide for customers looking to build an infrastructure that is optimized for virtualization, is highly available, is interoperable, and is efficient in terms of power and space consumption. It will explain the technologies used to build the infrastructure, provide use cases, and give guidance on deployments.

The essential reference for security pros and CCIE Security candidates: policies, standards, infrastructure/perimeter and content security, and threat protection Integrated Security Technologies and Solutions - Volume I offers one-stop expert-level instruction in security design, deployment, integration, and support methodologies to help security professionals manage complex solutions and prepare for their CCIE exams. It will help security pros succeed in their day-to-day jobs and also get ready for their CCIE Security written and lab exams. Part of the Cisco CCIE Professional Development Series from Cisco Press, it is authored by a team of CCIEs who are world-class experts in their Cisco security disciplines, including co-creators of the CCIE Security v5 blueprint. Each chapter starts with relevant theory, presents configuration examples and applications, and concludes with practical troubleshooting. Volume 1 focuses on security policies and standards; infrastructure security; perimeter security (Next-Generation Firewall, Next-Generation Intrusion Prevention Systems, and Adaptive Security Appliance [ASA]), and the advanced threat protection and content security sections of the CCIE Security v5 blueprint. With a strong focus on interproduct integration, it also shows how to combine formerly disparate systems into a seamless, coherent next-generation security solution. Review security standards, create security policies, and organize security with Cisco SAFE architecture Understand and mitigate threats to network infrastructure, and protect the three planes of a network device Safeguard wireless networks, and mitigate risk on Cisco WLC and access points Secure the network perimeter with Cisco Adaptive Security Appliance (ASA) Configure Cisco Next-Generation Firewall Firepower Threat Defense (FTD) and operate security via Firepower Management Center (FMC) Detect and prevent intrusions with Cisco Next-Gen IPS, FTD, and FMC Configure and verify Cisco IOS Firewall features such as ZBFW and address translation Deploy and configure the Cisco web and email security appliances to protect content and defend against advanced threats Implement Cisco Umbrella Secure Internet Gateway in the cloud as your first line of defense against internet threats Protect against new malware with Cisco Advanced Malware Protection and Cisco ThreatGrid

Cisco ASA for Accidental Administrators is a major update to the previous Accidental Administrator ASA book. This new edition is packed with 48 easy-to-follow hands-on exercises to help you build a working firewall configuration from scratch. Based on software version 9.x, it continues as the most straight-forward approach to learning how to configure the Cisco ASA Security Appliance, filled with practical tips and secrets learned from years of teaching and consulting on the ASA. There is no time wasted on boring theory. The essentials are covered in chapters on installing, backups and restores, remote administration, VPNs, DMZs, userames, transparent mode, static NAT, port address translation, access lists, DHCP, password recovery, logon banners, AAA (authentication, authorization and accounting), filtering content and more. Inside this concise, step-by-step guide, you’ll find: \*\*How to backup and restore software images and configurations \*\*How to configure different types of VPNs, including AAA authentication \*\*The secrets to successfully building and implementing access-lists All this information is presented in a straight-forward style that you can understand and use right away. The idea is for you to be able to sit down with your ASA and build a working configuration in a matter of minutes. Of course, some of the more advanced configs may take a little longer, but even so, you’ll be able to “get it done” in a minimal amount of time!

CCNA Security 640-554 Official Cert Guide

Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security

CCNP Security Firewall 642-618 Official Cert Guide

An Illustrated Step-By-Step ASA Learning and Configuration Guide

All-in-one Next-Generation Firewall, IPS, and VPN Services

All-in-one Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance

Cisco ASA, PIX, and FWSM Firewall HandbookPearson Education

Cisco’s ASA All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition Identify, mitigate, and respond to today’s highly-sophisticated network attacks. Today, network attackers are far more sophisticated, relentless, and dangerous. In response, Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services has been fully updated to cover the newest techniques and Cisco technologies for maximizing end-to-end security in your environment. Three leading Cisco security experts guide you through every step of creating a complete security plan with Cisco ASA, and then deploying, configuring, operating, and troubleshooting your solution. Fully updated for today’s newest ASA releases, this edition adds new coverage of ASA 5500-X, ASA 5585-X, ASA Services Module, ASA next-generation firewall services, EtherChannel, Global ACLs, clustering, IPv6 improvements, IKEv2, AnyConnect Secure Mobility VPN clients, and more. The authors explain significant recent licensing changes; introduce enhancements to ASA IPS; and walk you through configuring IPsec, SSL VPN, and NAT/PAT. You’ll learn how to apply Cisco ASA adaptive identification and mitigation services to systematically strengthen security in network environments of all sizes and types. The authors present up-to-date sample configurations, proven design scenarios, and actual debugs—all designed to help you make the most of Cisco ASA in your rapidly evolving network. Jazil Frattin, CCIE® No. 5459 (Routing and Switching; Security), Principal Engineer in the Global Security Solutions team, guides Cisco customers in security-focused network design and implementation. He architects, develops, and launches new security services concepts. His books include Cisco SSL VPN Solutions and Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting. Omar Santos, CISSP No. 46398, Cisco Product Security Incident Response Team (PSIRT) technical leader, leads and mentors engineers and incident managers in investigating and resolving vulnerabilities in Cisco products and protecting Cisco customers. Through 18 years in IT and cybersecurity, he has designed, implemented, and supported numerous secure networks for Fortune® 500 companies and the U.S. government. He is also the author of several other books and numerous whitepapers and articles. Andrew Ossipov, CCIE® No. 18483 and CISSP No. 344324, is a Cisco Technical Marketing Engineer focused on firewalls, intrusion prevention, and data center security. Drawing on more than 16 years in networking, he works to solve complex customer technical problems, and define future directions for Cisco’s product portfolio. He holds several pending patents. Understand, install, configure, license, maintain, and troubleshoot the newest ASA devices Efficiently implement Authentication, Authorization, and Accounting (AAA) services Control and provision network access with packet filtering, context-aware Cisco ASA next-generation firewall services, and new NAT/PAT concepts Configure IP routing, application inspection, and QoS Create firewall contexts with unique configurations, interfaces, policies, routing tables, and administration Enable integrated protection against many types of malware and advanced persistent threats (APTs) via Cisco Cloud Web Security and Cisco Security Intelligence Operations (SIO) Implement high availability with failover and elastic scalability with clustering Deploy, troubleshoot, monitor, tune, and manage Intrusion Prevention System (IPS) features Implement site-to-site IPsec VPNs and all forms of remote-access VPNs (IPsec, clientless SSL, and client-based SSL) Configure and troubleshoot Public Key Infrastructure (PKI) Use IKEv2 to more effectively resist attacks against VPNs Leverage IPv6 support for IPS, packet inspection, transparent firewalls, and site-to-site IPsec VPNs

Trust the best selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for exam success. They are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. CCNP Security FIREWALL 642-618 Official Cert Guide presents you with an organized test preparation routine through the use of proven series elements and techniques. “Do I Know This Already?” quizzes open each chapter and enable you to decide how much time you need to spend on each section. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. · Master Cisco CCNP Security FIREWALL exam topics · Assess your knowledge with chapter-opening quizzes · Review key concepts with exam preparation tasks · Practice with realistic exam questions on the CD-ROM CCNP Security FIREWALL 642-618 Official Cert Guide, focuses specifically on the objectives for the CCNP Security FIREWALL exam. Expert networking consultants Dave Hucabay, Dave Garneau, and Anthony Sequeira share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The companion CD-ROM contains a powerful Pearson IT Certification Practice Test engine that enables you to focus on individual topic areas or take a complete, timed exam. The assessment engine also tracks your performance and provides feedback on a module-by-module basis, laying out a complete assessment of your knowledge to help you focus your study where it is needed most. Well-regarded for its level of detail, assessment features, comprehensive design scenarios, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The official study guide helps you master all the topics on the CCNP Security FIREWALL exam, including: ASA interfaces IP connectivity ASA management Recording ASA activity Address translation Access control Proxy services Traffic inspection and handling Transparent firewall mode Virtual firewalls High availability ASA service modules CCNP Security FIREWALL 642-618 Official Cert Guide is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining. The print edition of the CCNP Security FIREWALL 642-618 Official Cert Guide contains a free, complete practice exam. Also available from Cisco Press for Cisco CCNP Security study is the CCNP Security FIREWALL 642-618 Official Cert Guide Premium Edition eBook and Practice Test. This digital-only certification preparation product combines an eBook with enhanced Pearson IT Certification Practice Test. This integrated learning package: · Allows you to focus on individual topic areas or take complete, timed exams · Includes direct links from each question to detailed tutorials to help you understand the concepts behind the questions · Provides unique sets of exam-realistic practice questions · Tracks your performance and provides feedback on a module-by-module basis, laying out a complete assessment of your knowledge to help you focus your study where it is needed most

The official, comprehensive assessment, review, and practice guide for Cisco’s latest CCNP Security Firewall exam – direct from Cisco \* Covers every new Cisco Firewall exam topic, including connectivity, Cisco ASA management, activity recording, address translation, access control, proxy services, traffic inspection, QoS, virtual firewalls, high availability, and service module integration. \*CD contains realistic practice tests. \*Extensive, proven features help students review efficiently and remember key details. This is Cisco’s official, comprehensive self-study resource for preparing for the new CCNP Security Firewall exam, one of the four required exams for CCNP Security certification. Designed for intermediate-to-advanced level readers, it covers every objective concisely and logically, with extensive teaching features designed to promote retention and understanding. Readers will find: \* Pre-chapter quizzes to assess knowledge upfront and focus study more efficiently. \*Foundation topics sections that explain concepts and configurations, and link theory to actual configuration commands. \*Key topics sections calling attention to every figure, table, and list that candidates must know. \*Exam Preparation sections with additional chapter review features. \*Final preparation chapter providing tools and a complete final study plan. \*Customizable practice test library on CD-ROM This book’s comprehensive coverage includes: \* Understanding and working with Cisco ASA. \*Deploying basic and IP connectivity. \*Managing ASAs and recording their activities. \*Using address translation. \*Controlling access and inspecting traffic. \*Using Proxy services to control access. \*Controlling Quality of Service (QoS). \*Creating Virtual Firewalls. \*Deploying high availability features. \*Integrating ASA Service Modules

Computer Security

Automating Cisco Security Solutions SAUTO (300-735) Exam Practice Questions & Dumps

Cisco Network Security Troubleshooting Handbook

CCNP Security FIREWALL 642-617 Official Cert Guide

Securing Cisco IP Telephony Networks

CCNP Security Firewall 642-617 Official Cert Guide

Identify, analyze, and resolve current and potential network security problems Learn diagnostic commands, common problems and resolutions, best practices, and case studies covering a wide array of Cisco network security troubleshooting scenarios and products Refer to common problems and resolutions in each chapter to identify and solve chronic issues or expedite escalation of problems to the Cisco TAC/HTTS Flip directly to the techniques you need by following the modular chapter organization Isolate the components of a complex network problem in sequence Master the troubleshooting techniques used by TAC/HTTS security support engineers to isolate problems and resolve them on all four security domains: IDS/IPS, AAA, VPNs, and firewalls With the myriad Cisco® security products available today, you need access to a comprehensive source of defensive troubleshooting strategies to protect your enterprise network. Cisco Network Security Troubleshooting Handbook can single-handedly help you analyze current and potential network security problems and identify viable solutions, detailing each step until you reach the best resolution. Through its modular design, the book allows you to move between chapters and sections to find just the information you need. Chapters open with an in-depth architectural look at numerous popular Cisco security products and their packet flows, while also discussing potential third-party compatibility issues. By following the presentation of troubleshooting techniques and tips, you can observe and analyze problems through the eyes of an experienced Cisco TAC or High-Touch Technical Support (HTTS) engineer or determine how to your case to a TAC/HTTS engineer. Part I starts with a solid overview of troubleshooting tools and methodologies. In Part II, the author explains the features of Cisco ASA and Cisco PIX® version 7.0 security platforms, Firewall Services Module (FWSM), and Cisco IOS® firewalls. Part III covers troubleshooting IPsec Virtual Private Networks (IPsec VPN) on Cisco IOS routers, Cisco PIX firewalls with embedded VPN functionalities, and the Cisco 3000 Concentrator. Troubleshooting tools and techniques on the Authentication, Authorization, and Accounting (AAA) framework are discussed through routers, Cisco PIX firewalls, and Cisco VPN 3000 concentrators in Part IV. Part IV also covers troubleshooting Cisco Secure ACS on Windows, the server-side component of the AAA framework. IDS/IPS troubleshooting · Deployments of voice over IP (VoIP) networks continue at a rapid pace. Voice gateways are an essential part of VoIP networks, handling the many tasks involved in translating between transmission formats and protocols and acting as the interface between an IP telephony network and the PSTN or PBX. Gatekeepers and IP-to-IP gateways help these networks scale. Gatekeepers provide call admission control, call routing, address resolution, and bandwidth management between H.323 endpoints including Cisco IOS® voice gateways and Cisco® Unified CallManagers. IP-to-IP gateways allow VoIP calls to traverse disparate IP networks. Cisco Voice Gateways and Gatekeepers provides detailed solutions to real-world problems encountered when implementing a VoIP network. This practical guide helps you understand Cisco gateways and gatekeepers and configure them properly. Gateway selection, design issues, feature configuration, and security and high-availability issues are all covered in depth. The abundant examples, screen shots, configuration snips, and case studies make this a truly practical and useful guide: anyone interested in the proper implementation of gateways and gatekeepers in a VoIP network. Emphasis is placed on the accepted best practices and common issues encountered in real-world deployments. Cisco Voice Gateways and Gatekeepers is divided into four parts. Part I provides an overview of an IP voice network. Part II is dedicated to voice gateways, including discussions of Media Gateway Control Protocol (MGCP). Part II.3:23: Session Initiation Protocol (SIP)· voice circuit options; connecting to the PSTN, PBX, and IP WAN; dial plans; digit manipulation; selection; class of restriction; Survivable Remote Site Telephony (SRST) and MGCP fallback; digital signal processor (DSP) resources; and Tool Command Language (Tcl) scripts and Voice XML (VXML). Part III addresses voice gatekeepers, including detailed deployment and configuration. Part IV is dedicated to IP-to-IP gateways. This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book. The Firewall Services Module (FWSM) is a high-performance stateful-inspection firewall that integrates into the Cisco® 6500 switch and 7600 router chassis. The FWSM monitors traffic flows using application inspection engines to provide a strong level of network security. The FWSM defines the security parameter and enables the enforcement of security policies through authentication, access control and protocol inspection. The FWSM is a key component of any other deploying network security. Cisco Secure Firewall Services Module (FWSM) covers all aspects of the FWSM. The book provides a detailed look at how the FWSM processes information, as well as installation, configuration details, recommendations for network integration, and reviews of operation and management. This book provides you with a single source that comprehensively answers how and why the FWSM functions as it does. This information enables you to successfully deploy th

FWSM and gain the greatest functional benefit from your deployment. Practical examples throughout show you how other customers have successfully deployed the FWSM. By reading this book, you will learn how the FWSM functions, the differences between the FWSM and the ASA Security Appliance, how to implement and maintain the FWSM, the latest features of the FWSM, and how to configure common installations. 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.

Cisco® ASA All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition Identify, mitigate, and respond to today's highly-sophisticated network attacks. Today, network attackers are far more sophisticated, relentless, and dangerous. In response, Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services has been fully updated to cover the newest techniques and Cisco technologies for maximizing end-to-end security in your environment. Three leading Cisco security experts guide you through every step of creating a complete security plan with Cisco ASA, and then deploying, configuring, operating, and troubleshooting your solution. Fully updated for today's newest ASA releases, this edition adds new coverage of ASA 5500-X, ASA 5585-X, ASA Services Module, ASA next-generation firewall services, EtherChannel, Global ACLs, clustering, IPv6 improvements, IKEv2, AnyConnect Secure Mobility VPN clients, and more. The authors explain significant recent licensing changes, introduce enhancements to ASA IPS, and walk you through configuring IPsec, SSL VPN, and NAT/PAT. You'll learn how to apply Cisco ASA adaptive identification and mitigation services to systematically strengthen security in network environments of all sizes and types. The authors present up-to-date sample configurations, proven design scenarios, and actual debugs— all designed to help you make the most of Cisco ASA in your rapidly evolving network. Jazib Frahim, CCIE® No. 5459 (Routing and Switching; Security), Principal Engineer in the Global Security Solutions team, guides top-tier Cisco customers in security-focused network design and implementation. He architects, develops, and launches new security services concepts. His books include Cisco SSL VPN Solutions and Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting. Omar Santos, CISSP No. 463598, Cisco Product Security Incident Response Team (PSIRT) technical leader, leads and mentors engineers and incident managers in investigating and resolving vulnerabilities in Cisco products and protecting Cisco customers. Through 18 years in IT and cybersecurity, he has designed, implemented, and supported numerous secure networks for Fortune® 500 companies and the U.S. government. He is also the author of several other books and numerous whitepapers and articles. Andrew Ossipov, CCIE® No. 18483 and CISSP No. 344324, is a Cisco Technical Marketing Engineer focused on firewalls, intrusion prevention, and data center security. Drawing on more than 16 years in networking, he works to solve complex customer technical problems, architect new features and products, and define future directions for Cisco's product portfolio. He holds several pending patents. Understand, install, configure, license, manage, and troubleshoot the newest ASA devices Efficiently implement Authentication, Authorization, and Accounting (AAA) services Control and provision network access with packet filtering, context-aware Cisco ASA next-generation firewall services, and new NAT/PAT concepts Configure IP routing, application inspection, and QoS Create firewall contexts with unique configurations, interfaces, policies, routing tables, and administration Enable integrated protection against many types of malware and advanced persistent threats (APTs) via Cisco Cloud Web Security and Cisco Security Intelligence Operations (SIO) Implement high availability with failover and elastic scalability with clustering Deploy, troubleshoot, monitor, tune, and manage Intrusion Prevention System (IPS) features Implement site-to-site IPsec VPNs and all forms of remote-access VPNs (IPsec, clientless SSL, and client-based SSL) Configure and troubleshoot Public Key Infrastructure (PKI) Use IKEv2 to more effectively resist attacks against VPNs Leverage IPv6 support for IPS, packet inspection, transparent firewalls, and site-to-site IPsec VPNs CCNA Security 210-260 Certification Guide Cisco ISE for BYOD and Secure Unified Access

Cisco Voice Gateways and Gatekeepers  
Cisco Secure Firewall Services Module (FWSM)

CCNA Security Study Guide  
This is the only book available on building network DMZs, which are the cornerstone of any good enterprise security configuration. It covers market-leading products from Microsoft, Cisco, and Check Point. One of the most complicated areas of network technology is designing, planning, implementing, and constantly maintaining a demilitarized zone (DMZ) segment. This book is divided into four logical parts. First the reader will learn the concepts and major design principles of all DMZs. Next the reader will learn how to configure the actual hardware that makes up DMZs for both newly constructed and existing networks. Next, the reader will learn how to securely populate the DMZs with systems and services. The last part of the book deals with troubleshooting, maintaining, testing, and implementing security on the DMZ. The only book published on Network DMZs on the components of securing enterprise networks This is the only book available on building network DMZs, which are the cornerstone of any good enterprise security configuration. It covers market-leading products from Microsoft, Cisco, and Check Point Provides detailed examples for building Enterprise DMZs from the ground up and retro-fitting existing infrastructures

Your first step into the world of network security No security experience required Includes clear and easily understood explanations Makes learning easy Your first step to network security begins here! Learn about hackers and their attacks Understand security tools and technologies Defend your network with firewalls, routers, and other devices Explore security for wireless networks Learn how to prepare for security incidents Welcome to the world of network security! Computer networks are indispensable-but they're also not secure. With the proliferation of Internet viruses and worms, many people and companies are considering increasing their network security. But first, you need to make sense of this complex world of hackers, viruses, and the tools to combat them. No security experience needed! Network Security First-Step explains the basics of network security in easy-to-grasp language that all of us can understand. This book takes you on a guided tour of the core technologies that make up and control network security. Whether you are looking to take your first step into a career in network security or are interested in simply gaining knowledge of the technology, this book is for you!

This is the eBook version of the printed book. If the print book includes a CD-ROM, this content is not included within the eBook version. For organizations of all sizes, the Cisco ASA product family offers powerful new tools for maximizing network security. Cisco ASA: All-in-One Firewall, IPS, Anti-X and VPN Adaptive Security Appliance, Second Edition, is Cisco's authoritative practitioner's guide to planning, deploying, managing, and troubleshooting security with Cisco ASA. Written by two leading Cisco security experts, this book presents each Cisco ASA solution in depth, offering comprehensive sample configurations, proven troubleshooting methodologies, and debugging examples. Readers will learn about the Cisco ASA Firewall solution and capabilities; secure configuration and troubleshooting of site-to-site and remote access VPNs; Intrusion Prevention System features built into Cisco ASA's Advanced Inspection and Prevention Security Services Module (AIP-SSM); and Anti-X features in the ASA Content Security and Control Security Services Module (CSC-SSM). This new edition has been updated with detailed information on the latest ASA models and features. Everything network professionals need to know to identify, mitigate, and respond to network attacks with Cisco ASA Includes detailed configuration examples, with screenshots and command line references Covers the ASA 8.2 release Presents complete troubleshooting methodologies and architectural references

Developed in collaboration with a training and certification team from Cisco, Computer Network Security is an exploration of the state-of-the-art and good practices in setting up a secure computer system. Concrete examples are offered in each chapter, to help the reader to master the concept and apply the security configuration. This book is intended for students preparing for the CCNA Security Exam (210-260 IINS) ? whether at professional training centers, technical faculties, or training centers associated with the Cisco Academy program. It is also relevant to anyone interested in computer security, be they professionals in this field or users who want to identify the threats and vulnerabilities of a network to ensure better security.

All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance  
Designing and Building Enterprise DMZs  
IKEv2 IPsec Virtual Private Networks

Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS

Day One

CCNP Security FIREWALL 642-618 Quick Reference

This book serves as a guide to help the reader develop an awareness of security vulnerabilities and attacks, and encourages them to be circumspect when using the various computer resources and tools available today. For experienced users, Computer Science Security presents a wide range of tools to secure legacy software and hardware. Computing has infiltrated all fields nowadays. No one can escape this wave and be immune to security attacks, which continue to evolve, gradually reducing the level of expertise needed by hackers. It is high time for each and every user to acquire basic knowledge of computer security, which would enable them to mitigate the threats they may face both personally and professionally. It is this combined expertise of individuals and organizations that will guarantee a minimum level of security for families, schools, the workplace and society in general.

Annotation: Cisco® ASA All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition Identify, mitigate, and respond to today's highly-sophisticated network attacks. Today, network attackers are far more sophisticated, relentless, and dangerous. In response, Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services has been fully updated to cover the newest techniques and Cisco technologies for maximizing end-to-end security in your environment. Three leading Cisco security experts guide you through every step of creating a complete security plan with Cisco ASA, and then deploying, configuring, operating, and troubleshooting your solution. Fully updated for today's newest ASA releases, this edition adds new coverage of ASA 5500-X, ASA 5585-X, ASA Services Module, ASA next-generation firewall services, EtherChannel, Global ACLs, clustering, IPv6 improvements, IKEv2, AnyConnect Secure Mobility VPN clients, and more. The authors explain significant recent licensing changes, introduce enhancements to ASA IPS, and walk you through configuring IPsec, SSL VPN, and NAT/PAT. You'll learn how to apply Cisco ASA adaptive identification and mitigation services to systematically strengthen security in network environments of all sizes and types. The authors present up-to-date sample configurations, proven design scenarios, and actual debugs—all designed to help you make the most of Cisco ASA in your rapidly evolving network. Jazib Frahim, CCIE® No. 5459 (Routing and Switching; Security), Principal Engineer in the Global Security Solutions team, guides top-tier Cisco customers in security-focused network design and implementation. He architects, develops, and launches new security services concepts. His books include Cisco SSL VPN Solutions and Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting. Omar Santos, CISSP No. 463598, Cisco Product Security Incident Response Team (PSIRT) technical leader, leads and mentors engineers and incident managers in investigating and resolving vulnerabilities in Cisco products and protecting Cisco customers. Through 18 years in IT and cybersecurity, he has designed, implemented, and supported numerous secure networks for Fortune®500 companies and the U.S. government. He is also the author of several other books and numerous whitepapers and articles. Andrew Ossipov, CCIE® No. 18483 and CISSP No. 344324, is a Cisco Technical Marketing Engineer focused on firewalls, intrusion prevention, and data center security. Drawing on more than 16 years in networking, he works to solve complex customer technical problems, architect new features and products, and define future directions for Cisco's product portfolio. He holds several pending patents. Understand, install, configure, license, maintain, and troubleshoot the newest ASA devices Efficiently implement Authentication, Authorization, and Accounting (AAA) services Control and provision network access with packet filtering, context-aware Cisco ASA next-generation firewall services, and new NAT/PAT concepts Configure IP routing, application inspection, and QoS Create firewall contexts with unique configurations, interfaces, routing tables, and administration

Cisco Security Specialist's Guide to PIX Firewall immerses the reader in the highly complicated subject of firewall implementation, deployment, configuration, and administration. This guide will instruct the reader on the necessary information to pass the CSPFA exam including protocols, hardware, software, troubleshooting and more. Cisco Security Specialist's Guide to PIX Firewall introduces the basic concepts of attack, explains the networking principals necessary to effectively implement and deploy a PIX firewall, covers the hardware and software components of the device, provides multiple configurations and administration examples, and fully describes the unique line syntax native to PIX firewall configuration and administration. Coverage of the Latest Versions of PIX Firewalls. This book includes coverage of the latest additions to the PIX Firewall family including the CiscoSecure PIX Firewall (PIX) Software Release 6.0 Must-have desk reference for the serious security professional. In addition to the foundation information and dedicated text focused on the exam objectives for the CSPFA, this book offers real-world administration and configuration support. This book will not only help readers pass the exam; it will continue to assist them with their duties on a daily basis Firewall administration guides? Syngress wrote the book. Syngress has demonstrated a proficiency to answer the market need for quality information pertaining to firewall administration guides. Configuring ISA Server 2000: Building Firewalls for Windows 2000 (ISBN: 1-928994-29-6) and Checkpoint Next Generation Security Administration (ISBN: 1-928994-74-1) are currently best sellers in the security market.

Fully updated: The complete guide to Cisco Identity Services Engine solutions Using Cisco Secure Access Architecture and Cisco Identity Services Engine, you can secure and gain control of access to your networks in a Bring Your Own Device (BYOD) world. This second edition of Cisco ISE for BYOD and Secure Unified Accesscontains more than eight brand-new chapters as well as extensively updated coverage of all the previous topics in the first edition book to reflect the latest technologies, features, and best practices of the ISE solution. It begins by reviewing today's business case for identity solutions. Next, you walk through ISE foundational topics and ISE design. Then you explore how to build an access security policy using the building blocks of ISE. Next are the in-depth and advanced ISE configuration sections, followed by the troubleshooting and monitoring chapters. Finally, we go in depth on the new TACACS+ device administration solution that is new to ISE and to this second edition. With this book, you will gain an understanding of ISE configuration, such as identifying users, devices, and security posture; learn about Cisco Secure Access solutions; and master advanced techniques for securing access to networks, from dynamic segmentation to guest access and everything in between. Drawing on their cutting-edge experience supporting Cisco enterprise customers, the authors offer in-depth coverage of the complete lifecycle for all relevant ISE solutions, making this book a cornerstone resource whether you're an architect, engineer, operator, or IT manager. · Review evolving security challenges associated with borderless networks, ubiquitous mobility, and consumerized IT · Understand Cisco Secure Access, the Identity Services Engine (ISE), and the building blocks of complete solutions · Design an ISE-enabled network, plan/distribute ISE functions, and prepare for rollout · Build context-aware security policies for network access, devices, accounting, and audit · Configure device profiles, visibility, endpoint posture assessments, and guest services · Implement secure guest lifecycle management, from WebAuth to sponsored guest access · Configure ISE, network access devices, and supplicants, step by step · Apply best practices to avoid the pitfalls of BYOD secure access · Set up efficient distributed ISE deployments · Provide remote access VPNs with ASA and Cisco ISE · Simplify administration with self-service onboarding and registration · Deploy security group access with Cisco TrustSec · Prepare for high availability and disaster scenarios · Implement passive identities via ISE-PIC and EZ Connect · Implement TACACS+ using ISE · Monitor, maintain, and troubleshoot ISE and your entire Secure Access system · Administer device AAA with Cisco IOS, WLC, and Nexus

Integrated Security Technologies and Solutions - Volume I

All-in-one Next-generation Firewall, IPS, and VPN Services

AAA Identity Management Security

Cisco Asa Firewall Fundamentals

Exam 45 Official Cert OdePub

Exam 640-553

Learn about network security, including the threats and the ways a network is protected from them. The book also covers firewalls, viruses and virtual private networks.

This is the eBook version of the printed book. The eBook does not contain the practice test software that accompanies the print book. CCNP Security FIREWALL 642-617 Official Cert Guide is a best of breed Cisco exam study guide that focuses specifically on the objectives for the CCNP Security FIREWALL exam. Senior security consultants and instructors David Hucaby, Dave Garneau, and Anthony Sequeira share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. Learn, prepare, and practice for exam success Master CCNP Security FIREWALL 642-617 exam topics Assess your knowledge with chapter-opening quizzes Review key concepts with exam preparation tasks CCNP Security FIREWALL 642-617 Official Cert Guide presents you with an organized test-preparation routine through the use of proven services elements and techniques. "Do I Know This Already?" quizzes open each chapter and enable you to decide how much time you need to spend on each section. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. CCNP Security FIREWALL 642-617 Official Cert Guide is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit [www.cisco.com/go/authorizedtraining](http://www.cisco.com/go/authorizedtraining). The official study guide helps you master all the topics on the CCNP Security FIREWALL exam, including ASA interfaces IP connectivity ASA management Recording ASA activity Address translation Access control Proxy services Traffic inspection and handling Transparent firewall mode Virtual firewalls High availability ASA service modules This volume is part of the Official Cert Guide Series from Cisco Press. Books in this series provide officially developed exam preparation materials that offer assessment, review, and practice to help Cisco Career Certification candidates identify weaknesses, concentrate their study efforts, and enhance their confidence as exam day nears.

A complete study guide for the new CCNA Security certification exam In keeping with its status as the leading publisher of CCNA study guides, Sybex introduces the complete guide to the new CCNA security exam. The CCNA Security certification is the first step towards Cisco's new Cisco Certified Security Professional (CCSP) and Cisco Certified Internetworking Engineer-Security. CCNA Security Study Guide fully covers every exam objective. The companion CD includes the Sybex Test Engine, flashcards, and a PDF of the book. The CCNA Security certification is the first step toward Cisco's new CCSP and Cisco Certified Internetworking Engineer-Security Describes security threats facing modern network infrastructures and how to mitigate threats to Cisco routers and networks using ACLs Explores implementing AAA on Cisco routers and secure network management and reporting Shows how to implement Cisco IOS Firewall and IPS Feature sets plus site-to-site VPNs using SDM CD includes the Sybex Test Engine, flashcards, and the book in PDF format With hands-on labs and end-of-chapter reviews, CCNA Security Study Guide thoroughly prepares you for certification. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

and the building blocks of complete solutions · Design an ISE-enabled network, plan/distribute ISE functions, and prepare for rollout · Build context-aware security policies for network access, devices, accounting, and audit · Configure device profiles, visibility, endpoint posture assessments, and guest services · Implement secure guest lifecycle management, from WebAuth to sponsored guest access · Configure ISE, network access devices, and supplicants, step by step · Apply best practices to avoid the pitfalls of BYOD secure access · Set up efficient distributed ISE deployments · Provide remote access VPNs with ASA and Cisco ISE · Simplify administration with self-service onboarding and registration · Deploy security group access with Cisco TrustSec · Prepare for high availability and disaster scenarios · Implement passive identities via ISE-PIC and EZ Connect · Implement TACACS+ using ISE · Monitor, maintain, and troubleshoot ISE and your entire Secure Access system · Administer device AAA with Cisco IOS, WLC, and Nexus

Verify firewall operation and connectivity and observe data passing through a firewall Configure Security Services Modules, such as the Content Security Control (CSC) module and the Advanced Inspection Processor (AIP) module 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: Cisco ASA 8.0, PIX 6.3, and FWSM 3.2 version firewalls

Help for Network Administrators

Cisco Security Specialists Guide to PIX Firewall

Exam Practice Questions For Automating Cisco Security Solutions SAUTO (300-735) Latest Version

Migrating from Cisco to Juniper Networks

Step-by-Step Practical Configuration Guide Using the Cli for Asa V8.x and V9.x

Network Security First-Step

Create and manage highly-secure IPsec VPNs with IKEv2 and Cisco FlexVPN The IKEv2 protocol significantly improves VPN security, and Cisco's FlexVPN offers a unified paradigm and command line interface for taking full advantage of it. Simple and modular, FlexVPN relies extensively on tunnel interfaces while maximizing compatibility with legacy VPNs. Now, two Cisco network security experts offer a complete, easy-to-understand, and practical introduction to IKEv2, modern IPsec VPNs, and FlexVPN. The authors explain each key concept, and then guide you through all facets of FlexVPN planning, deployment, migration, configuration, administration, troubleshooting, and optimization. You'll discover how IKEv2 improves on IKEv1, master key IKEv2 features, and learn how to apply them with Cisco FlexVPN. IKEv2 IPsec Virtual Private Networks offers practical design examples for many common scenarios, addressing IPv4 and IPv6, servers, clients, NAT, pre-shared keys, resiliency, overhead, and more. If you're a network engineer, architect, security specialist, or VPN administrator, you'll find all the knowledge you need to protect your organization with IKEv2 and FlexVPN. Understand IKEv2 improvements: anti-DDoS cookies, configuration payloads, acknowledged responses, and more Implement modern secure VPNs with Cisco IOS and IOS-XE Plan and deploy IKEv2 in diverse real-world environments Configure IKEv2 proposals, policies, profiles, keyrings, and authorization Use advanced IKEv2 features, including SGT transportation and IKEv2 fragmentation Understand FlexVPN, its tunnel interface types, and IOS AAA infrastructure Implement FlexVPN Server with EAP authentication, pre-shared keys, and digital signatures Deploy, configure, and customize FlexVPN clients Configure, manage, and troubleshoot the FlexVPN Load Balancer Improve FlexVPN resiliency with dynamic tunnel source, backup peers, and backup tunnels Monitor IPsec VPNs with AAA, SNMP, and Syslog Troubleshoot connectivity, tunnel creation, authentication, authorization, data encapsulation, and overlay routing Calculate IPsec overhead and fragmentation Plan your IKEv2 migration: hardware, VPN technologies, routing, restrictions, capacity, PKI, authentication, availability, and more

Thoroughly revised and expanded, this second edition adds sections on MPLS, Security, IPv6, and IP Mobility and presents solutions to the most common configuration problems.

"Richard Deal's gift of making difficult technology concepts understandable has remained constant. Whether it is presenting to a room of information technology professionals or writing books, Richard's communication skills are unsurpassed. As information technology professionals we are faced with overcoming challenges every day...Cisco ASA Configuration is a great reference and tool for answering our challenges." --From the Foreword by Steve Marincik (CCIE 7225), Systems Engineer, Cisco Systems A hands-on guide to implementing Cisco ASA Configure and maintain a Cisco ASA platform to meet the requirements of your security policy. Cisco ASA Configuration shows you how to control traffic in the corporate network and protect it from internal and external threats. This comprehensive resource covers the latest features available in Cisco ASA version 8.0, and includes detailed examples of complex configurations and troubleshooting. Implement and manage Cisco's powerful, multifunction network adaptive security appliance with help from this definitive guide. Configure Cisco ASA using the command-line interface (CLI) and Adaptive Security Device Manager (ASDM) Control traffic through the appliance with access control lists (ACLs) and object groups Filter Java, ActiveX, and web content Authenticate and authorize connections using Cut-through Proxy (CTP) Use Modular Policy Framework (MPF) to configure security appliance features Perform protocol and application inspection Enable IPsec site-to-site and remote access connections Configure WebVPN components for SSL VPN access Implement advanced features, including the transparent firewall, security contexts, and failover Detect and prevent network attacks Prepare and manage the AIP-SSM and CSC-SSM cards

The definitive insider's guide to planning, installing, configuring, and maintaining the new Cisco Adaptive Security Appliance.

Cisco ASA, PIX, and FWSM Firewall Handbook