Cisco Secure Perimeter Asa Acs Nexus Firesight Firepower Cisco Pocket Lab Guides Book 5

Eventually, you will certainly discover a further experience and talent by spending more cash. yet when? pull off you bow to that you require to get those every needs past having significantly cash? Why don't you try to get something basic in the beginning? That's something that will lead you to comprehend even more vis--vis the globe, experience, some places, following history, amusement, and a lot more?

It is your entirely own era to perform reviewing habit. in the course of guides you could enjoy now is **cisco secure perimeter asa acs nexus firesight firepower cisco pocket lab guides book 5** below.

TACACS+ \u0026 RADIUS Configuration on ACS for Cisco ASA   *An Overview of Cisco ACS*

How to Use Access-Lists on a Cisco ASA Security Appliance: Cisco ASA Training 101 How to Configure an ASA VPN Split-Tunnel: Cisco ASA Training 101 *Cisco ASA AAA Configuration with ACS - Authentication and Authorization*

LabMinutes# SEC0086 - Cisco ACS 5.4 TACACS Device Admin on Switch and ASA (Part 1) *INE Live Webinar : Understanding and Implementing NAT on Cisco ASA Firewall The Cisco ASA Security Appliance Eight Basic Configuration Commands: Cisco ASA Training 101*

How to Configure Static NAT on a Cisco ASA: Cisco ASA Training 101 *How to Set up a Cisco ASA DMZ: Cisco ASA Training 101 Cisco Security Webinar: Cisco ASA with FirePOWER* How to Reset Cisco ASA Passwords: Cisco ASA Training 101 **Cisco ASA Security Zones (Part 1) - Lecture # 2 - Doctor Networks Series \"Cisco ASA Fundamentals\"** **MicroNugget: How to Use ASA Firewall Packet Capture** 03 Understanding Security Zones \u0026 features in Cisco ASA MicroNugget: How to Control Traffic Filtering ACLs on the ASA Cisco ASA - Remote Access VPN (IPSec) *MicroNugget: What are the Different Static Routes on the ASA? Security - Configuring ASA Multiple Context Mode* Understanding Security Levels on Cisco ASA Firewall Tutorial : Cisco Training Videos cisco ASA ASDM Port forwarding on Version 9 MicroNugget: How to Configure NAT (PAT) on Cisco Routers Configuring Access Control Lists (ACL) | Cisco ASA Firewalls Cisco ASA - Twice NAT | Configuring Twice NAT | CCIE Security How to Use Active Directory and LDAP to Authenticate Cisco ASA VPN Users: Cisco ASA Training 101 Cisco ASA 5505 Firewall Initial Setup: Cisco ASA Training 101 *How to Perform Cisco ASA Remote Management using Telnet, SSH, and ASDM: Cisco ASA Training 101 The Accidental Administrator: Cisco ASA Security Appliance book trailer* **How to Use Active Directory and RADIUS to Authenticate Cisco ASA VPN Users: Cisco ASA Training 101 Cisco ASA SSL VPN with ACS and Introduction to Certificate (Day 52) Cisco Secure Perimeter Asa Acs**

Transparent mode and routed mode ASA contexts. Cisco ASA FirePOWER modules in all ASA firewalls to provide intrusion prevention (IPS). FirePOWER management using a FireSIGHT manager. Authentication, authorization and accounting for the entire system using Cisco ACS. All of this has been tested and is working in a real life environment in England UK.

Cisco Secure Perimeter: ASA - ACS - Nexus - FireSIGHT ...

Cisco Secure Perimeter book. Read reviews from world's largest community for readers. This book aims to provide the reader with the information needed to...

Cisco Secure Perimeter: ASA - ACS - Nexus - FireSIGHT ...

ASDM Procedure. Complete these steps in order to configure the ASA for authentication from the ACS server: Choose Configuration > Device Management > Users/AAA > AAA Server Groups > Add in order to create an AAA Server Group. Provide the AAA Server Group details in the Add AAA Server Group window as shown.

ASA 8.3: TACACS Authentication using ACS 5.X - Cisco

Configure Cisco Secure ACS and TACACS+. Verify TACACS+. This chapter looks at the features and architecture of the Cisco Secure Access Control Server (ACS) application. The chapter also covers the general process of preparing to install and configure the current versions of ACS support for Windows 2000/NT and UNIX (Solaris).

Chapter 4: Cisco Secure ACS and TACACS+/RADIUS ...

Cisco Secure Access Control System (ACS) allows you to centrally manage access to your network services and resources (including devices, such as IP phones, printers, and so on). ACS 5.7 is a policy-based access control system that allows you to create complex policy conditions and helps you to comply with the various Governmental regulations.

User Guide for Cisco Secure Access Control System 5.7 ...

Complete Steps 1 through 12 of the Configure ACS for Downloadable ACL for Individual User and perform these steps in order to configure Downloadable ACL for a Network Device Group in a Cisco Secure ACS. In this example, the RADIUS Client (ASA) belongs to the Network Device Group VPN-Gateways.The VPN authentication request coming from ASA for user "cisco" authenticates successfully, and the RADIUS server sends a downloadable access list to the security appliance. The user "cisco" can access ...

ASA 8.3 and Later: Radius Authorization (ACS 5.x ... - Cisco

This package covers use cases for Cisco Secure Access Control Server (ACS) that is an access policy control platform. Main Use Cases . Below are the main use cases for this packages: Cisco Secure ACS Account Harvesting Attempt Cisco Secure ACS Brute Force Attempt Cisco Secure ACS Successful Login Supported Log Sources

PCiscoSecureACS < ArcSightActivate < Foswiki

Cisco Secure ACS Express 5.0 is available as a one RU, security-hardened appliance with a preinstalled Cisco Secure ACS Express license. Cisco Secure ACS Express 5.0 supports a maximum of 50 AAA clients and 350 unique user logins in a 24-hour period. The following are some of the hardware specifications of Cisco Secure ACS Express 5.0:

Cisco Ebook: Chapter 02: Perimeter Security (Part04)

ACS is 1 Active directory domain per node. Here are the difference between ACS and ISE from security, eco-system support, interoperability with Cisco devices (Cisco on Cisco) and third party functionalities.

ACS vs ISE Comparison - Cisco Community

INTRODUCTION : #1 Cisco Secure Perimeter Asa Acs Publish By Louis L Amour, Amazoncom Cisco Secure Perimeter Asa Acs Nexus cisco secure perimeter asa acs nexus firesight firepower cisco pocket lab guides book 5 kindle edition by grant wilson author visit amazons grant wilson page find all the books read about the author and

30 E-Learning Book Cisco Secure Perimeter Asa Acs Nexus ...

Sep 05, 2020 cisco secure perimeter asa acs nexus firesight firepower cisco pocket lab guides book 5 Posted By James PattersonMedia Publishing TEXT ID 38731e64 Online PDF Ebook Epub Library 30 E Learning Book Cisco Secure Perimeter Asa Acs Nexus

101+ Read Book Cisco Secure Perimeter Asa Acs Nexus ...

Sep 07, 2020 cisco secure perimeter asa acs nexus firesight firepower cisco pocket lab guides book 5 Posted By Seiichi MorimuraPublic Library TEXT ID 38731e64 Online PDF Ebook Epub Library 30 Cisco Secure Perimeter Asa Acs Nexus Firesight

20 Best Book Cisco Secure Perimeter Asa Acs Nexus ...

Sep 27, 2020 cisco secure perimeter asa acs nexus firesight firepower cisco pocket lab guides book 5 Posted By Mary Higgins ClarkLibrary TEXT ID 38731e64 Online PDF Ebook Epub Library CISCO SECURE PERIMETER ASA ACS NEXUS FIRESIGHT FIREPOWER CISCO

Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide Second Edition Foundation learning for the CCNA Security IINS 640-554 exam Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, is a Cisco-authorized, self-paced learning tool for CCNA®Security 640-554 foundation learning. This book provides you with the knowledge needed to secure Cisco®networks. By reading this book, you will gain a thorough understanding of how to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. This book focuses on using Cisco IOS routers to protect the network by capitalizing on their advanced features as a perimeter router, firewall, intrusion prevention system, and site-to-site VPN device. The book also covers the use of Cisco Catalyst switches for basic network security, the Cisco Secure Access Control System (ACS), and the Cisco Adaptive Security Appliance (ASA). You learn how to perform basic tasks to secure a small branch office network using Cisco IOS security features available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and ASAs. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, 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. -- Develop a comprehensive network security policy to counter threats against information security -- Secure borderless networks -- Learn how to use Cisco IOS Network Foundation Protection (NFP) and Cisco Configuration Professional (CCP) -- Securely implement the management and reporting features of Cisco IOS devices -- Deploy Catalyst Switch security features -- Understand IPv6 security features -- Plan threat control strategies -- Filter traffic with access control lists -- Configure ASA and Cisco IOS zone-based firewalls -- Implement intrusion prevention systems (IPS) and network address translation (NAT) -- Secure connectivity with site-to-site IPsec VPNs and remote access VPNs This volume is in the Foundation Learning Guide Series offered by Cisco Press® These guides are developed together with Cisco as the only authorized, self-paced learning tools that help networking professionals build their understanding of networking concepts and prepare for Cisco certification exams. Category: Cisco Certification Covers: CCNA Security IINS exam 640-554

Implementing Cisco IOS Network Security (IINS) is a Cisco-authorized, self-paced learning tool for CCNA®Security foundation learning. This book provides you with the knowledge needed to secure Cisco®routers and switches and their associated networks. By reading this book, you will gain a thorough understanding of how to troubleshoot and monitor network devices to maintain integrity, confidentiality, and availability of data and devices, as well as the technologies that Cisco uses in its security infrastructure. This book focuses on the necessity of a comprehensive security policy and how it affects the posture of the network. You will learn how to perform basic tasks to secure a small branch type office network using Cisco IOS®security features available through the Cisco Router and Security Device Manager (SDM) web-based graphical user interface (GUI) and through the command-line interface (CLI) on Cisco routers and switches. The author also provides, when appropriate, parallels with Cisco ASA appliances. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) 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. Develop a comprehensive network security policy to counter threats against information security Configure routers on the network perimeter with Cisco IOS Software security features Configure firewall features including ACLs and Cisco IOS zone-based policy firewalls to perform basic security operations on a network Configure site-to-site VPNs using Cisco IOS features Configure IPS on Cisco network routers Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic This volume is in the Certification Self-Study Series offered by Cisco Press® Books in this series provide officially developed self-study solutions to help networking professionals understand technology implementations and prepare for the Cisco Career Certifications examinations.

End-to-End Network Security Defense-in-Depth Best practices for assessing and improving network defenses and responding to security incidents Omar Santos Information security practices have evolved from Internet perimeter protection to an in-depth defense model in which multiple countermeasures are layered throughout the infrastructure to address vulnerabilities and attacks. This is necessary due to increased attack frequency, diverse attack sophistication, and the rapid nature of attack velocity—all blurring the boundaries between the network and perimeter. End-to-End Network Security is designed to counter the new generation of complex threats. Adopting this robust security strategy defends against highly sophisticated attacks that can occur at multiple locations in your network. The ultimate goal is to deploy a set of security capabilities that together create an intelligent, self-defending network that identifies attacks as they occur, generates alerts as appropriate, and then automatically responds. End-to-End Network Security provides you with a comprehensive look at the mechanisms to counter threats to each part of your network. The book starts with a review of network security technologies then covers the six-step methodology for incident response and best practices from proactive security frameworks. Later chapters cover wireless network security, IP telephony security, data center security, and IPv6 security. Finally, several case studies representing small, medium, and large enterprises provide detailed example configurations and implementation strategies of best practices learned in earlier chapters. Adopting the techniques and strategies outlined in this book enables you to prevent day-zero attacks, improve your overall security posture, build strong policies, and deploy intelligent, self-defending networks. " Within these pages, you will find many practical tools, both process related and technology related, that you can draw on to improve your risk mitigation strategies." —Bruce Murphy, Vice President, World Wide Security Practices, Cisco Omar Santos is a senior network security engineer at Cisco® Omar has designed, implemented, and supported numerous secure networks for Fortune 500 companies and the U.S. government. Prior to his current role, he was a technical leader within the World Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations. Guard your network with firewalls, VPNs, and intrusion prevention systems Control network access with AAA Enforce security policies with Cisco Network Admission Control (NAC) Learn how to perform risk and threat analysis Harden your network infrastructure, security policies, and procedures against security threats Identify and classify security threats Trace back attacks to their source Learn how to best react to security incidents Maintain visibility and control over your network with the SAVE framework Apply Defense-in-Depth principles to wireless networks, IP telephony networks, data centers, and IPv6 networks 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: Network security and incident response

Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide Second Edition Foundation learning for the CCNA Security IINS 640-554 exam Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, is a Cisco-authorized, self-paced learning tool for CCNA®Security 640-554 foundation learning. This book provides you with the knowledge needed to secure Cisco®networks. By reading this book, you will gain a thorough understanding of how to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. This book focuses on using Cisco IOS routers to protect the network by capitalizing on their advanced features as a perimeter router, firewall, intrusion prevention system, and site-to-site VPN device. You learn how to perform basic tasks to secure a small branch office network using Cisco IOS security features available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and ASAs. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, 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. -- Develop a comprehensive network security policy to counter threats against information security -- Secure borderless networks -- Learn how to use Cisco IOS Network Foundation Protection (NFP) and Cisco Configuration Professional (CCP) -- Securely implement the management and reporting features of Cisco IOS devices -- Deploy Catalyst Switch security features -- Understand IPv6 features -- Plan threat control strategies -- Filter traffic with access control lists -- Configure ASA and Cisco IOS zone-based firewalls -- Implement intrusion prevention systems (IPS) and network address translation (NAT) -- Secure connectivity with site-to-site IPsec VPNs and remote access VPNs This volume is in the Foundation Learning Guide Series offered by Cisco Press® These guides are developed together with Cisco as the only authorized, self-paced learning tools that help networking professionals build their understanding of networking concepts and prepare for Cisco certification exams. Category: Cisco Certification Covers: CCNA Security IINS exam 640-554

As a final exam preparation tool, CCIE Security Exam Quick Reference Sheets provide a concise review of all objectives on the new CCIE Security written exam (350-018). This digital Short Cut 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 security and application protocols, security technologies, Cisco security applications, router and switch security, and security policy best practices. These fact-filled Quick Reference Sheets allow 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.

As a final exam preparation tool, CCIE Security v3.0 Quick Reference provides a concise review of all objectives on the CCIE Security written exam v3.0 (350-018). 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 security protocols, encryption, application protocols, security technologies, Cisco IOS security features, Cisco ASA, security management, wireless security, IPv6 security, security policies, network attack mitigation, and computer forensics . 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.

Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide Second Edition Foundation learning for the CCNA Security IINS 640-554 exam Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, is a Cisco-authorized, self-paced learning tool for CCNA ®Security 640-554 foundation learning. This book provides you with the knowledge needed to secure Cisco ® networks. By reading this book, you will gain a thorough understanding of how to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. This book focuses on using Cisco IOS routers to protect the network by capitalizing on their advanced features as a perimeter router, firewall, intrusion prevention system, and site-to-site VPN device. The book also covers the use of Cisco Catalyst switches for basic network security, the Cisco Secure Access Control System (ACS), and the Cisco Adaptive Security Appliance (ASA). You learn how to perform basic tasks to secure a small branch office network using Cisco IOS security features available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and ASAs. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, 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. -- Develop a comprehensive network security policy to counter threats against information security -- Secure borderless networks -- Learn how to use Cisco IOS Network Foundation Protection (NFP) and Cisco Configuration Professional (CCP) -- Securely implement the management and reporting features of Cisco IOS devices -- Deploy Catalyst Switch security features -- Understand IPv6 features -- Plan threat control strategies -- Filter traffic with access control lists -- Configure ASA and Cisco IOS zone-based firewalls -- Implement intrusion prevention systems (IPS) and network address translat ...

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 dog 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.

CCIE Professional Development Network Security Technologies and Solutions A comprehensive, all-in-one reference for Cisco network security Yusuf Bhaiji, CCIE No. 9305 Network Security Technologies and Solutions is a comprehensive reference to the most cutting-edge security products and methodologies available to networking professionals today. This book helps you understand and implement current, state-of-the-art network security technologies to ensure secure communications throughout the network infrastructure. With an easy-to-follow approach, this book serves as a central repository of security knowledge to help you implement end-to-end security solutions and provides a single source of knowledge covering the entire range of the Cisco network security portfolio. The book is divided into five parts mapping to Cisco security technologies and solutions: perimeter security, identity security and access management, data privacy, security monitoring, and security management. Together, all these elements enable dynamic links between customer security policy, user or host identity, and network infrastructures. With this definitive reference, you can gain a greater understanding of the solutions available and learn how to build integrated, secure networks in today's modern, heterogeneous networking environment. This book is an excellent resource for those seeking a comprehensive reference on mature and emerging security tactics and is also a great study guide for the CCIE Security exam. "Yusuf's extensive experience as a mentor and advisor in the security technology field has honed his ability to translate highly technical information into a straight-forward, easy-to-understand format. If you're looking for a truly comprehensive guide to network security, this is the one! " –Steve Gordon, Vice President, Technical Services, Cisco Yusuf Bhaiji, CCIE No. 9305 (R&S and Security), has been with Cisco for seven years and is currently the program manager for Cisco CCIE Security certification. He is also the CCIE Proctor in the Cisco Dubai Lab. Prior to this, he was technical lead for the Sydney TAC Security and VPN team at Cisco. Filter traffic with access lists and implement security features on switches Configure Cisco IOS router firewall features and deploy ASA and PIX Firewall appliances Understand attack vectors and apply Layer 2 and Layer 3 mitigation techniques Secure management access with AAA Secure access control using multifactor authentication technology Implement identity-based network access control Apply the latest wireless LAN security solutions Enforce security policy compliance with Cisco NAC Learn the basics of cryptography and implement IPsec VPNs, DMVPN, GET VPN, SSL VPN, and MPLS VPN technologies Monitor network activity and security incident response with network and host intrusion prevention, anomaly detection, and security monitoring and correlation Deploy security management solutions such as Cisco Security Manager, SDM, ADSM, PDM, and IDM Learn about regulatory compliance issues such as GLBA, HIPPA, and SOX This book is part of the Cisco CCIE Professional Development Series from Cisco Press, which offers expert-level instruction on network design, deployment, and support methodologies to help networking professionals manage complex networks and prepare for CCIE exams. Category: Network Security Covers: CCIE Security Exam

Reduce the threat of network attacks with an authorized self-study guide One of the primary components of any organization's security policy is the implementation and maintenance of firewalls. Firewalls are network devices residing at the perimeter of corporate networks that protect internal networks from intrusion by the outside world. The integrated hardware/software PIX Firewall series delivers high security without impacting network performance while scaling to meet the entire range of customer requirements. Based on the official instructor-led training course (Cisco Secure PIX Firewall Advanced-CSPFA), Cisco Secure PIX Firewalls teaches you the skills needed to describe, configure, verify, and manage the PIX Firewall product family and the Cisco IOS(r) Firewall feature set. Starting with a discussion of hacking methodologies and internal and external threats, this book opens by describing the Cisco Security Wheel, emphasizing network security as a continuous process. The authors then familiarize you with the characteristics of the various PIX models and examine upgrade tasks. This book covers basic installation details, as well as how to enable more advanced features and access control. In addition, this book details management and monitoring with PIX Syslog services and the PIX AAA subsystem. You also learn to configure the PIX Failover mechanism, IPSec on the PIX, and the Cisco IOS Firewall feature set. The appendixes provide helpful references, including configuring PIX intrusion detection features, SNMP management support, DHCP client and server, Secure Shell Protocol (SSH) connection, and dozens of security-related resources. Whether you are preparing for the Cisco Security Specialist 1 certification or simply want to understand and make the most efficient use of PIX Firewalls, Cisco Secure PIX Firewalls provides you with a complete solution for planning, deploying, and managing PIX Firewall protected networks. Prepare for the Cisco Security Specialist 1 PIX exam with the official CSPFA self-study guide Understand the physical characteristics of PIX models 506, 515, 520, 525, and 535, including LED information and port and slot numbering Upgrade PIX OS code, perform password recovery, and install feature licenses Configure IPSec Phase I and Phase II Security Associations Configure Cisco routers to perform Context Based Access Control (CBAC) Examine the many operating features of the PIX, such as Cut-Through Proxy, Advanced Protocol Handling, Attack Guards, and the Adaptive Security Algorithm (ASA) Learn the ins and outs of address translation and access control Install the Cisco Secure ACS server and configure corresponding services on the PIX to authenticate and authorize users and services Understand attack guards such as Syn Flood, Fragmentation, AAA, DNS, and Mail Examine the workings of the PIX failover mechanism and learn the difference between failover, stateful failover, interface testing, and the failover poll David W. Chapman Jr., CCNP(r), CCDP(r), CSS-1, is a Cisco Security Instructor with Global Knowledge. As Course Director for the Cisco Secure PIX Firewall course, David is charged with maintaining the integrity and quality of the course offering and mentoring instructors new to the course. Andy Fox, CCSI(tm), CCNA(r), CCDA(r), CSS-1 is a Certified Cisco Systems Instructor with Global Knowledge. Andy has been teaching Cisco Certified Classes for more than five years and is the Course Director for the Managing Cisco Network Security course.

Copyright code : 0ecc1571db28b66b3f97a0808757f17O