Cisco Firepower Threat Defense Software On Select Asa

Thank you unquestionably much for downloading **cisco firepower threat defense software on select asa**.Maybe you have knowledge that, people have see numerous times for their favorite books like this cisco firepower threat defense software on select asa, but end stirring in harmful downloads.

Rather than enjoying a fine ebook taking into account a mug of coffee in the afternoon, instead they juggled gone some harmful virus inside their computer. **cisco firepower threat defense software on select asa** is approachable in our digital library an online permission to it is set as public therefore you can download it instantly. Our digital library saves in combined countries, allowing you to get the most less latency era to download any of our books in the manner of this one. Merely said, the cisco firepower threat defense software on select asa is universally compatible afterward any devices to read.

Firepower Threat Defense - Common Practice Guide Walkthrough

~~Introduction to Cisco FTD Firepower Systems and installation~~ *1. Cisco Firepower Threat Defense: Convert ASA to FTD 2. Cisco Firepower Threat Defense: Firepower Device Manager (Base Configuration)* ~~3. Cisco Firepower Threat Defense: Quick Installation Firepower Management Center~~ *1. Cisco Firepower Threat Defense 6.2.2: Firepower Device Manager (VM Initial Setup Script)* ~~2. Cisco Firepower Threat Defense 6.2.2: Firepower Device Manager (Initial Setup GUI)~~ 14. Cisco Firepower Threat Defense: Malware Policy ~~20. Cisco Firepower Threat Defense: NGIPS Tuning Firepower Recommendation~~ ~~1. Cisco Firepower Threat Defense 6.3.0: Multi-Instance - Configuring Firepower 4110 Appliance~~ ~~Firepower Threat Defense Hidden CLI~~ 16. Cisco Firepower Threat Defense: IPS Policy Balanced ~~Cisco: Security - Firepower 4100 FXOS \u0026 Firmware Update~~ *Cisco ASA to FTD Migration Firepower 2100 Series Platform 2. Cisco Firepower Threat Defense: Quick Installation NGFW*

Cisco FirePOWER / Sourcefire Overview - Todd Lammle Training Series *Cisco Firepower NGFW Portfolio Overview* Cisco Firepower (FTD) CLISH and Lina Mode ~~Cisco Firepower - Introduction, Configuration, and Best Practice | Webinar~~

Installing ASA on Firepower 2100 platform*Monitoring and Reporting with Firepower Device Manager* ~~Overview firepower threat defense~~ **2. Cisco Firepower Threat Defense 6.3.0: Multi-Instance - Configuring Mult-**

Instance *38. Cisco Firepower Threat Defense: Inline Set IPS (Routed Mode)*

Cisco's Firepower Management Center API*Firepower Threat Defense (FTD) : Intermediate Configuration* ~~12. Cisco Firepower Threat Defense 6.3 Attack Series: Reporting~~ ~~Cisco Firepower Threat Defense 6.2.2: Some differences when leveraging Firepower~~ 10. Cisco Firepower Threat Defense 6.3 Attack Series: Detection and Analysis **Cisco Firepower Threat Defense Software**

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to upload arbitrary-sized files to specific folders on an affected device, which could lead to an unexpected device reload.

Cisco Adaptive Security Appliance Software and Firepower ...

A vulnerability in the FTP inspection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass FTP inspection. The vulnerability is due to ineffective flow tracking of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP traffic through an affected device.

Cisco Adaptive Security Appliance Software and Firepower ...

Summary. A vulnerability in the Clientless SSL VPN (WebVPN) of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to inject arbitrary HTTP headers in the responses of the affected system. The vulnerability is due to improper input sanitization.

Cisco Adaptive Security Appliance Software and Firepower ...

Cisco Firepower Threat Defense (FTD) is an integrative software image combining CISCO ASA and FirePOWER feature into one hardware and software inclusive system. Cisco is a pioneer in the Next ...

What is Cisco Firepower Threat Defense (FTD)?

A vulnerability in the IP fragment-handling implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device.

Cisco Adaptive Security Appliance Software and Firepower ...

Book Title. Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.7 . Chapter Title. Remote Access VPN. PDF - Complete Book (37.62 MB) PDF - This Chapter (2.42 MB) View

with Adobe Reader on a variety of devices

Cisco Firepower Threat Defense Configuration Guide for ...

A vulnerability in the TCP packet processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory exhaustion condition.

Cisco Adaptive Security Appliance Software and Firepower ...

A vulnerability in the SSL/TLS session handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory leak when closing SSL/TLS connections in a specific state.

Cisco Adaptive Security Appliance Software and Firepower ...

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and obtain read and delete access

to sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of the HTTP URL.

Cisco Adaptive Security Appliance Software and Firepower ...

A vulnerability in the DHCP module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. The vulnerability is due to incorrect processing of certain DHCP packets. An attacker could exploit this vulnerability by sending a crafted ...

Cisco Adaptive Security Appliance Software and Firepower ...

A vulnerability in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their Cisco FTD instance and execute commands with root privileges in the host namespace. The attacker must have valid credentials on the device. The vulnerability exists because a configuration file that is used at container ...

Cisco Firepower Threat Defense Software Multi-Instance ...

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Denial of Service Vulnerability 23-Oct-2020; Cisco

Adaptive Security Appliance Software and Firepower Threat Defense Software for Firepower 1000/2100 Series Appliances Secure Boot Bypass Vulnerabilities 23-Oct-2020

Cisco Firepower 2110 Security Appliance - Cisco

A vulnerability in the TCP Intercept functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured Access Control Policies (including Geolocation) and Service Polices on an affected system. The vulnerability exists because TCP Intercept is invoked when the embryonic connection limit is reached, which can cause the underlying detection engine to process the packet incorrectly.

Cisco Firepower Threat Defense Software TCP Intercept ...

A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to access hidden commands. The vulnerability is due to the presence of undocumented configuration commands. An attacker could exploit this vulnerability by performing specific steps that make the hidden commands accessible. A successful exploit could allow the attacker to ...

Cisco Firepower Threat Defense Software Hidden Commands ...

A vulnerability in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their Cisco FTD instance and execute commands with root privileges in the host namespace. The attacker must have valid credentials on the device.The vulnerability exists because a configuration file that is used at container ...

Cisco Firepower Threat Defense Software Multi-Instance ...

Download Software for Firepower Threat Defense (FTD) Download Software for Firepower Management Center (FMC) Compatibility Guides. ASA and FTD Compatibility Guides; ASA Compatibility Guide; Cisco Firepower 4100/9300 FXOS Compatibility ; PSIRT & Field Notice Security Advisory Page Security Advisories, Responses and Notices; Datasheets. Cisco ...

Cisco Firepower Threat Defense (FTD) - Cisco Community

Book Title. Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.1 . Chapter Title. System Management. PDF - Complete Book (9.18 MB) PDF - This Chapter (1.28 MB) View with Adobe Reader on a variety of devices

Cisco Firepower Threat Defense Configuration Guide for ...

Cisco has fixed 12 high-severity flaws in its Adaptive Security

Appliance software and Firepower Threat Defense software. Cisco has stomped out 12 high-severity vulnerabilities across several ...

Cisco Fixes High-Severity Flaws In Firepower Security ...

The majority of the bugs in Cisco's Firepower Threat Defense (FTD) and Adaptive Security Appliance (ASA) software can enable denial of service (DoS) on affected devices. Cisco has stomped out a ...

Network threats are emerging and changing faster than ever before. Cisco Next-Generation Network Security technologies give you all the visibility and control you need to anticipate and meet tomorrow's threats, wherever they appear. Now, three Cisco network security experts introduce these products and solutions, and offer expert guidance for planning, deploying, and operating them. The authors present authoritative coverage of Cisco ASA with FirePOWER Services; Cisco Firepower Threat Defense (FTD); Cisco Next-Generation IPS appliances; the Cisco Web Security Appliance (WSA) with integrated Advanced Malware Protection (AMP); Cisco Email Security Appliance (ESA) with integrated Advanced Malware Protection (AMP); Cisco AMP ThreatGrid Malware Analysis and Threat Intelligence, and the Cisco

Firepower Management Center (FMC). You'll find everything you need to succeed: easy-to-follow configurations, application case studies, practical triage and troubleshooting methodologies, and much more. Effectively respond to changing threat landscapes and attack continuums Design Cisco ASA with FirePOWER Services and Cisco Firepower Threat Defense (FTD) solutions Set up, configure, and troubleshoot the Cisco ASA FirePOWER Services module and Cisco Firepower Threat Defense Walk through installing AMP Private Clouds Deploy Cisco AMP for Networks, and configure malware and file policies Implement AMP for Content Security, and configure File Reputation and File Analysis Services Master Cisco AMP for Endpoints, including custom detection, application control, and policy management Make the most of the AMP ThreatGrid dynamic malware analysis engine Manage Next-Generation Security Devices with the Firepower Management Center (FMC) Plan, implement, and configure Cisco Next-Generation IPS—including performance and redundancy Create Cisco Next-Generation IPS custom reports and analyses Quickly identify the root causes of security problems

The authoritative visual guide to Cisco Firepower Threat Defense (FTD) This is the definitive guide to best practices and advanced troubleshooting techniques for the Cisco flagship Firepower Threat

Defense (FTD) system running on Cisco ASA platforms, Cisco Firepower security appliances, Firepower eXtensible Operating System (FXOS), and VMware virtual appliances. Senior Cisco engineer Nazmul Rajib draws on unsurpassed experience supporting and training Cisco Firepower engineers worldwide, and presenting detailed knowledge of Cisco Firepower deployment, tuning, and troubleshooting. Writing for cybersecurity consultants, service providers, channel partners, and enterprise or government security professionals, he shows how to deploy the Cisco Firepower next-generation security technologies to protect your network from potential cyber threats, and how to use Firepower's robust command-line tools to investigate a wide variety of technical issues. Each consistently organized chapter contains definitions of keywords, operational flowcharts, architectural diagrams, best practices, configuration steps (with detailed screenshots), verification tools, troubleshooting techniques, and FAQs drawn directly from issues raised by Cisco customers at the Global Technical Assistance Center (TAC). Covering key Firepower materials on the CCNA Security, CCNP Security, and CCIE Security exams, this guide also includes end-of-chapter quizzes to help candidates prepare. · Understand the operational architecture of the Cisco Firepower NGFW, NGIPS, and AMP technologies · Deploy FTD on ASA platform and Firepower appliance running FXOS · Configure and troubleshoot Firepower

Management Center (FMC) · Plan and deploy FMC and FTD on VMware virtual appliance · Design and implement the Firepower management network on FMC and FTD · Understand and apply Firepower licenses, and register FTD with FMC · Deploy FTD in Routed, Transparent, Inline, Inline Tap, and Passive Modes · Manage traffic flow with detect-only, block, trust, and bypass operations · Implement rate limiting and analyze quality of service (QoS) · Blacklist suspicious IP addresses via Security Intelligence · Block DNS queries to the malicious domains · Filter URLs based on category, risk, and reputation · Discover a network and implement application visibility and control (AVC) · Control file transfers and block malicious files using advanced malware protection (AMP) · Halt cyber attacks using Snort-based intrusion rule · Masquerade an internal host's original IP address using Network Address Translation (NAT) · Capture traffic and obtain troubleshooting files for advanced analysis · Use command-line tools to identify status, trace packet flows, analyze logs, and debug messages

This book is written like a learning course, explained in detail with a lab topology using FTDv and FMCv. Hence this is a 100% practical guide on configuring and managing Cisco Firepower Threat Defense Next Generation Firewall using Cisco Firepower Management Center. I have

also covered the standalone firewall introduction and how to use Firepower Device Manager to manage your FTD firewall locally without using FMC.Covers,*How to upgrade ASA firewall to Cisco FTD (Migration and Upgrade)*Configure Cisco Firepower Thread Defence (FTD) Next Generation firewall*Configure Cisco Firepower Management Center (FMC)*Manage and administer the FTD devices using FMC (Configure interfaces, zones, routing, ACLs, Prefilter policies, NAT, High Availability etc)* FTD local management using Firepower Device Manager (FDM)*Introduction to the FTD Migration toolTable of Contents*Introduction*How to use this book?*What is Cisco FTD?*Lab Topology*Setting up Cisco Firepower Threat Defense (FTD) Firewall*Changing Management IP*Configure Manager in Cisco FTD*Setting up Cisco Firepower Management Center (FMC)*License Activation*Explore the Cisco FMC options*Register Cisco FTD with Cisco FMC*Configure the Firewall Zone and Interface*Additional Notes on Sub-Interface and Redundant Interfaces*Create a Platform Policy*Configure Routing on Cisco FTD*Configuring FTD as a DHCP server*Network Address Translation (NAT)*Create an Access Control Policy*Pre-Filter Policy*Configuring High Availability on Cisco FTD*Upgrading Cisco ASA firewall to FTD*Installing Cisco FTD image on an existing ASA Firewall*Install Firepower Threat Defense System Software*Manage Cisco FTD firewall using Firepower Device Manager (FDM)*Bonus: Introduction to Cisco FTD

migration toolNote: This book doesn't cover the topics on VPN, SGT, and Cisco ISE integration.

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

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 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 topic 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 --Bring 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 IPS 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.

This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CCNA Cyber Ops SECFND 210-250 exam success with this Cert Guide from Pearson IT Certification, a leader in IT Certification learning. Master CCNA Cyber Ops SECFND 210-250 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks CCNA Cyber Ops SECFND 210-250 Official Cert Guide is a best-of-breed exam study guide. Cisco enterprise security experts Omar Santos, Joseph Muniz, and Stefano De Crescenzo 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 book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy.

Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. The study guide helps you master all the topics on the CCNA Cyber Ops SECFND exam, including: Fundamentals of networking protocols and networking device types Network security devices and cloud services Security principles Access control models Security management concepts and techniques Fundamentals of cryptography and PKI Essentials of Virtual Private Networks (VPNs) Windows-based Analysis Linux /MAC OS X-based Analysis Endpoint security technologies Network and host telemetry Security monitoring operations and challenges Types of attacks and vulnerabilities Security evasion techniques

Cisco has announced big changes to its certification program. As of February 24, 2020, all current certifications will be retired, and Cisco will begin offering new certification programs. The good news is if you’re working toward any current CCNA certification, keep going.

You have until February 24, 2020 to complete your current CCNA. If you already have CCENT/ICND1 certification and would like to earn CCNA, you have until February 23, 2020 to complete your CCNA certification in the current program. Likewise, if you're thinking of completing the current CCENT/ICND1, ICND2, or CCNA Routing and Switching certification, you can still complete them between now and February 23, 2020. Up the ante on your FirePOWER with Advanced FireSIGHT Administration exam prep Securing Cisco Networks with Sourcefire IPS Study Guide, Exam 500-285, provides 100% coverage of the FirePOWER with Advanced FireSIGHT Administration exam objectives. With clear and concise information regarding crucial next-generation network security topics, this comprehensive guide includes practical examples and insights drawn from real-world experience, exam highlights, and end of chapter reviews. Learn key exam topics and powerful features of the Cisco FirePOWER Services, including FireSIGHT Management Center, in-depth event analysis, IPS tuning and configuration, and snort rules language. Gain access to Sybex's superior online learning environment that includes practice questions, flashcards, and interactive glossary of terms. Use and configure next-generation Cisco FirePOWER services, including application control, firewall, and routing and switching capabilities Understand how to accurately tune your systems to improve performance and network intelligence while leveraging powerful tools

for more efficient event analysis Complete hands-on labs to reinforce key concepts and prepare you for the practical applications portion of the examination Access Sybex's online interactive learning environment and test bank, which includes an assessment test, chapter tests, bonus practice exam questions, electronic flashcards, and a searchable glossary Securing Cisco Networks with Sourcefire IPS Study Guide, Exam 500-285 provides you with the information you need to prepare for the FirePOWER with Advanced FireSIGHT Administration examination.

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, 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 Cisco Firepower SNCF 300-710 Official Cert Guide presents you with an organized test preparation routine using proven series elements and techniques. "Do I Know This Already?" quizzes open each chapter and allow 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 CCNP Security Securing Networks with Cisco Firepower (SNCF 300-710) exam topics Assess your knowledge with chapter-opening quizzes Review key concepts with exam preparation tasks Practice with realistic exam questions in the practice test software CCNP Security Cisco Firepower SNCF 300-710 Official Cert Guide, from Cisco Press allows you to succeed on the exam the first time and is the only self-study resource approved by Cisco. Author Nazmul Rajib shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual

knowledge and hands-on skills. This complete study package includes A test-preparation routine proven to help you pass the exams Do I Know This Already? quizzes, which allow you to decide how much time you need to spend on each section Chapter-ending and part-ending exercises, which help you drill on key concepts you must know thoroughly Study plan suggestions and templates to help you organize and optimize your study time Well regarded for its level of detail, study plans, assessment features, challenging review questions and exercises, and video instruction, this official study guide helps you master the concepts and techniques that ensure your exam success. This official study guide helps you master all the topics on the Securing Networks with Cisco Firepower (SNCF 300-710) exam, including Policy configurations Integrations Deployments Management and troubleshooting

This book is focused on Firepower essentials. In it, you will find practical, best practice recommendations for configuring and using Firepower. Each best practice is listed in the table of contents so you can quickly find it along with an explanation of why it is important. Essential Firepower will help you learn how to effectively configure and use this system, what is important, and what is not. The best way to use this book is to read each of the recommendations with their associated explanation and decide if they are right for you. Not

every recommendation will be applicable to your Firepower deployment. However, you will find that most will provide valuable real-world information and insight into the type of tuning that will bring out the true value and potential of your Firepower system. The goal of this book is not to be just another tome on the switches, knobs and dials available to configure and tune the Firepower NGFW. The primary focus is to provide pragmatic, real-life information and advice to network and security administrators who use this system day-to-day. You will get the benefit of the author's 14 years of experience as a user, instructor and consultant with the Sourcefire 3D and FireSIGHT/Firepower system. If you are ready to learn the practical application of Firepower technology, and to gain understanding you won't get from the official documentation, then this book is for you.