

Palo Alto Firewall Cli Guide

Personal data in the online world as become a commodity. Coveted by criminals, demanded by governments, and used for unsavory purposes by marketers and advertisers, your private information is at risk everywhere. For libraries and librarians, this poses a professional threat as well as a personal one. How can we protect the privacy of library patrons and users who browse our online catalogs, borrow sensitive materials, and use our public computers and networks? User Privacy: A Practical Guide for Librarians answers that question. Through simple explanations and detailed, step-by-step guides, library professionals will learn how to strengthen privacy protections for: Library policies Wired and wireless networks Public computers Web browsers Mobile devices Apps Cloud computing Each chapter begins with a "threat assessment" that provides an overview of the biggest security risks - and the steps that can be taken to deal with them. Also covered are techniques for preserving online anonymity, protecting activists and at-risk groups, and the current state of data encryption.

How do you tailor education to the learning needs of adults? Do they learn differently from children? How does their life experience inform their learning processes? These were the questions at the heart of Malcolm Knowles' pioneering theory of andragogy which transformed education theory in the 1970s. The resulting principles of a self-directed, experiential, problem-centred approach to learning have been hugely influential and are still the basis of the learning practices we use today. Understanding these principles is the cornerstone of increasing motivation and enabling adult learners to achieve. The 9th edition of The Adult Learner has been revised to include: Updates to the book to reflect the very latest advancements in the field. The addition of two new chapters on diversity and inclusion in adult learning, and andragogy and the online adult learner. An updated supporting website. This website for the 9th edition of The Adult Learner will provide basic instructor aids. For each chapter, there will be a PowerPoint presentation, learning exercises, and added study questions. Revisions throughout to make it more readable and relevant to your practices. If you are a researcher, practitioner, or student in education, an adult learning practitioner, training manager, or involved in human resource development, this is the definitive book in adult learning you should not be without.

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

As one of the first books to distill the economics of information and networks into practical business strategies, this is a guide to the winning moves that can help business leaders--from writers, lawyers and finance professional to executives in the entertainment, publishing and hardware and software industries-- navigate successfully through the information economy.

An ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes

User Privacy

Cassandra: The Definitive Guide

Official Google Cloud Certified Associate Cloud Engineer Study Guide

The Adult Learner

A Practical Guide

Develop practical skills to perform pentesting and risk assessment of Microsoft Azure environments

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

Whether your network is a complex carrier or just a few machines supporting a small enterprise, JUNOS High Availability will help you build reliable and resilient networks that include Juniper Networks devices. With this book's valuable advice on software upgrades, scalability, remote network monitoring and management, high-availability protocols such as VRRP, and more, you'll have your network uptime at the five, six, or even seven nines -- or 99.99999% of the time. Rather than focus on "greenfield" designs, the authors explain how to intelligently modify multi-vendor networks. You'll learn to adapt new devices to existing protocols and platforms, and deploy continuous systems even when reporting scheduled downtime. JUNOS High Availability will help you save time and money. Manage network equipment with Best Common Practices Enhance scalability by adjusting network designs and protocols Combine the IGP and BGP networks of two merging companies Perform network audits Identify JUNOScripting techniques to maintain high availability Secure network equipment against breaches, and contain DoS attacks Automate network configuration through specific strategies and tools This book is a core part of the Juniper Networks Technical Library™.

The career of computer visionary Grace Murray Hopper, whose innovative work in programming laid the foundations for the user-friendliness of today's personal computers that sparked the information age. A Hollywood biopic about the life of computer pioneer Grace Murray Hopper (1906-1992) would go like this: a young professor abandons the ivy-covered walls of academia to serve her country in the Navy after Pearl Harbor and finds herself on the front lines of the computer revolution. She works hard to succeed in the all-male computer industry, is almost brought down by personal problems but survives them, and ends her career as a celebrated elder stateswoman of computing, a heroine to thousands, hailed as the inventor of computer programming. Throughout Hopper's later years, the popular media told this simplified version of her life story. In Grace Hopper and the Invention of the Information Age, Kurt Beyer reveals a more authentic Hopper, a vibrant and complex woman whose career paralleled the meteoric trajectory of the postwar computer industry. Both rebellious and collaborative, Hopper was influential in male-dominated military and business organizations at a time when women were encouraged to devote themselves to housework and childbearing. Hopper's greatest technical achievement was to create the tools that would allow humans to communicate with computers in terms other than ones and zeroes. This advance influenced all future programming and software design and laid the foundation for the development of user-friendly personal computers.

Use ACI fabrics to drive unprecedented value from your data center environment With the Cisco Application Centric Infrastructure (ACI) software-defined networking platform, you can achieve dramatic improvements in data center performance, redundancy, security, visibility, efficiency, and agility. In Deploying ACI, three leading Cisco experts introduce this breakthrough platform, and walk network professionals through all facets of design, deployment, and operation. The authors demonstrate how ACI changes data center networking, security, and management; and offer multiple field-proven configurations. Deploying ACI is organized to follow the key decision points associated with implementing data center network fabrics. After a practical introduction to ACI concepts and design, the authors show how to bring your fabric online, integrate virtualization and external connections, and efficiently manage your ACI network. You'll master new techniques for improving visibility, control, and availability; managing multitенancy; and seamlessly inserting service devices into application data flows. The authors conclude with expert advice for troubleshooting and automation, helping you deliver data center services with unprecedented efficiency. Understand the problems ACI solves, and how it solves them Design your ACI fabric, build it, and interface with devices to bring it to life Integrate virtualization technologies with your ACI fabric Perform networking within an ACI fabric (and understand how ACI changes data center networking) Connect external networks and devices at Layer 2/Layer 3 levels Coherently manage unified ACI networks with tenants and application policies Migrate to granular policies based on applications and their functions Establish multitенancy, and evolve networking, security, and services to support it Integrate L4-7 services: device types, design scenarios, and implementation Use multisite designs to meet rigorous requirements for redundancy and business continuity Troubleshoot and monitor ACI fabrics Improve operational efficiency through automation and programmability

InfoWorld

From Underground Sources

Fortinet Network Security Introduction

Understanding ArubaOS

The Protocols

Best Practices for High Network Uptime

Version 6. X

Learn to leverage the power of PowerCLI to automate your VMware vSphere environment with ease About This Book This is first book on the market that will enlighten you on the latest version of PowerCLI and how to implement it Effectively manage virtual machines, network comprehensive and practical book on automating VMware vSphere Who This Book Is For This book is ideal for you if you want to learn how to automate your VMware vSphere or vCloud infrastructure by getting the most out of PowerCLI. It's assumed that you have some experience with PowerCLI. Knowledge of Microsoft's Windows PowerShell is not a prerequisite. What You Will Learn Explore PowerShell and PowerCLI cmdlets and their output objects See how to manage virtual machines and work with virtual networks Manage vCloud Director from PowerCLI Create a disaster recovery solution Manage NSX and vRealize Automation using REST API with PowerCLI Create and configure vSphere HA and DRS clusters Use vSphere Update Manager with PowerCLI to create patch baselines and scan hosts Explore reporting techniques to use PowerCLI, a free extension to Microsoft Windows PowerShell, enables you to automate the management of a VMware vSphere or vCloud environment. This book will show you how to automate your tasks and make your job easier. Starting with an introduction to the basics of PowerCLI, you'll learn how to use PowerCLI to manage your vSphere and vCloud infrastructure from the command line. To help you manage a vSphere host overall, you will learn how to manage vSphere ESXi hosts, host profiles, host services, host firewall, and deploy and upgrade ESXi hosts using Image Builder and Auto Deploy. The book will also show you how to create datastore and datastore clusters, but you'll also work with profile-driven and policy-based storage to manage your storage. To create a disaster recovery solution and retrieve information from vRealize Operations, you will learn how to use Site Recovery Manager and vRealize Operations. You'll see how to use the REST APIs from PowerShell to manage NSX and vRealize Automation and create patch baselines, scan hosts against the baselines for missing patches, and re-mediate hosts. By the end of the book, you will be capable of using the best tool to automate your vSphere. Style and approach This comprehensive book will teach system administrators everything about PowerCLI 6 and how to utilize it to automate VMware vSphere.

Discover high-value Azure security insights, tips, and operational optimizations This book presents comprehensive Azure Security Center techniques for safeguarding cloud and hybrid environments. Leading Microsoft security and cloud experts Yuri Diogenes and Dr. Thomas Shindler provide a full spectrum of features and capabilities to address protection, detection, and response in key operational scenarios. You'll learn how to secure any Azure workload, and optimize virtually all facets of modern security, from policies and identity to incident response and risk management. You'll learn how to save hours, days, or even weeks by solving problems in most efficient, reliable ways possible. Two of Microsoft's leading cloud security experts show how to: • Assess the impact of cloud and hybrid environments on security, compliance, operations, data protection, and security paradigm for a world without traditional perimeters • Gain visibility and control to secure compute, network, storage, and application workloads • Incorporate Azure Security Center into your security operations center • Integrate Azure Security Center with Azure AD Identity Protection • Adapt Azure Security Center's built-in policies and definitions for your organization • Perform security assessments and implement Azure Security Center recommendations • Use incident response features to detect, investigate, and address threats • Create high-fidelity fusion of security issues • Implement application whitelisting and just-in-time VM access • Monitor user behavior and access, and investigate compromised or misused credentials • Customize and perform operating system security baseline assessments • Leverage integrated threat intelligence • Gain visibility into network traffic and identify suspicious activity Perspectives in Computing: A Computational Logic Handbook contains a precise description of the logic and a detailed reference guide to the associated mechanical theorem proving system, including a primer for the logic as a functional programming language, an introduction to the mechanical theorem. The publication first offers information on a primer for the logic, formalization within the logic, and a precise description of the logic. Discussions focus on induction and recursion, quantification, explicit value terms, dealing with features and omissions, element operators, and conventional data structures. The text then takes a look at proving theorems in the logic, mechanized proofs in the logic, and an introduction to the system. The text examines the processes involved in using the theorem prover, four classes of rules generated from Topics include executable counterparts, toggle, elimination of irrelevancy, heuristic use of equalities, representation of formulas, type sets, and the crucial check points in a proof attempt. The publication is a vital reference for researchers interested in computational logic.

Software Defined Networks: A Comprehensive Approach, Second Edition provides in-depth coverage of the technologies collectively known as Software Defined Networking (SDN). The book shows how to explain to business decision-makers the benefits and risks in shifting parts of a network, and how to develop or acquire SDN applications. In addition, the book emphasizes the parts of the technology that encourage opening up the network, providing treatment for alternative approaches to SDN that expand the definition of SDN as new existing solutions. Since the first edition was published, the SDN market has matured, and is being gradually integrated and morphed into something more compatible with mainstream networking vendors. This book reflects these changes, with coverage of the OpenDaylight controller, protocols, the inclusion of NETCONF in discussions on controllers and devices, expanded coverage of NFV, and updated coverage of the latest approved version (1.5.1) of the OpenFlow specification. Contains expanded coverage of controllers Includes a new chapter on NETCONF and its use in optical networks Provides support materials for use in computer networking courses

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

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

Cisco ASA for Accidental Administrators

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

Distributed Data at Web Scale

The Definitive Cybersecurity Guide for Directors and Officers

TCP/IP Illustrated, Volume 1

The Certified Network Security Engineer6 (PCNSE6) exam tests your knowledge of the core features and functions of Palo Alto Networks next-generation firewalls. It is especially useful for those leading or participating in projects. This certification includes all the questions you will face in the exam center. This certification is best for students who want to get deeper understanding on configuration Palo Alto Firewalls. Preparing for the Certified Network Security Engineer6 (PCNSE6) exam to become a certified Network Security Engineer6 (PCNSE6) expert by Palo Alto? Here we have brought Best Exam Questions for you so that you can prepare well for this Exam of Certified Network Security Engineer6 (PCNSE6). Unlike other online simulation practice tests, you get an ebook version that is easy to read & remember these questions. You can simply rely on these questions for successfully certifying this exam.

Learn how to defend your ICS in practice, from lab setup and intel gathering to working with SCADA Key FeaturesBecome well-versed with offensive ways of defending your industrial control systemsLearn about industrial network protocols, threat hunting, Active Directory compromises, SQL injection, and much moreBuild offensive and defensive skills to combat industrial cyber threatsBook Description The industrial cybersecurity domain has grown significantly in recent years. To completely secure critical infrastructure, red teams must be employed to continuously test and exploit the security integrity of a company's people, processes, and products. This is a unique pentesting book, which takes a different approach by helping you gain hands-on experience with equipment that you'll come across in the field. This will enable you to understand how industrial equipment interacts and operates within an operational environment. You'll start by getting to grips with the basics of industrial processes, and then see how to create and break the process, along with gathering open-source intel to create a threat landscape for your potential customer. As you advance, you'll find out how to install and utilize offensive techniques used by professional hackers. Throughout the book, you'll explore industrial equipment, port and service discovery, pivoting, and much more, before finally launching attacks against systems in an industrial network. By the end of this penetration testing book, you'll not only understand how to analyze and navigate the intricacies of an industrial control system (ICS), but you'll also have developed essential offensive and defensive skills to proactively protect industrial networks from modern cyberattacks. What you will learnSet up a starter-kit ICS lab with both physical and virtual equipmentPerform open source intel-gathering pre-engagement to help map your attack landscapeGet to grips with the Standard Operating Procedures (SOPs) for penetration testing on industrial equipmentUnderstand the principles of traffic spanning and the importance of listening to customer networksGain fundamental knowledge of ICS communicationConnect physical operational technology to engineering workstations and supervisory control and data acquisition (SCADA) softwareGet hands-on with directory scanning tools to map web-based SCADA solutionsWho this book is for If you are an ethical hacker, penetration tester, automation engineer, or IT security professional looking to maintain and secure industrial networks from adversaries, this book is for you. A basic understanding of cybersecurity and recent cyber events will help you get the most out of this book.

InfoWorld is targeted to Senior IT professionals. Content is segmented into Channels and Topic Centers. InfoWorld also celebrates people, companies, and projects.

Enhance Windows security and protect your systems and servers from various cyber attacks Key Features Protect your device using a zero-trust approach and advanced security techniques Implement efficient security measures using Microsoft Intune, Configuration Manager, and Azure solutions Understand how to create cyber-threat defense solutions effectively Book Description Are you looking for effective ways to protect Windows-based systems from being compromised by unauthorized users? Mastering Windows Security and Hardening is a detailed guide that helps you gain expertise when implementing efficient security measures and creating robust defense solutions. We will begin with an introduction to Windows security fundamentals, baselining, and the importance of building a baseline for an organization. As you advance, you will learn how to effectively secure and harden your Windows-based system, protect identities, and even manage access. In the concluding chapters, the book will take you through testing, monitoring, and security operations. In addition to this, you'll be equipped with the tools you need to ensure compliance and continuous monitoring through security operations. By the end of this book, you'll have developed a full understanding of the processes and tools involved in securing and hardening your Windows environment. What you will learn Understand baselining and learn the best practices for building a baseline Get to grips with identity management and access management on Windows-based systems Delve into the device administration and remote management of Windows-based systems Explore security tips to harden your Windows server and keep clients secure Audit, assess, and test to ensure controls are successfully applied and enforced Monitor and report activities to stay on top of vulnerabilities Who this book is for This book is for system administrators, cybersecurity and technology professionals, solutions architects, or anyone interested in learning how to secure their Windows-based systems. A basic understanding of Windows security concepts, Intune, Configuration Manager, Windows PowerShell, and Microsoft Azure will help you get the best out of this book.

Cisco ASA

A Comprehensive Approach

Practical techniques to enable and protect remote users, improve your security posture, and troubleshoot next-generation firewalls

Pentesting Industrial Control Systems

Deploying ACI

Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats

Cisco Asa Firewall Fundamentals

Explore everything you need to know to set up secure remote access, harden your firewall deployment, and protect against phishing Key FeaturesLearn the ins and outs of log forwarding and troubleshooting issuesSet up GlobalProtect satellite connections, configure site-to-site VPNs, and troubleshoot LSPN issuesGain an in-depth understanding of user credential detection to prevent data leaks Book Description This book builds on the content found in Mastering Palo Alto Networks, focusing on the different methods of establishing remote connectivity, automating log actions, and protecting against phishing attacks through user credential detection. Complete with step-by-step instructions, practical examples, and troubleshooting tips, you will gain a solid understanding of how to configure and deploy Palo Alto Networks remote access products. As you advance, you will learn how to design, deploy, and troubleshoot large-scale end-to-end user VPNs. Later, you will explore new features and discover how to incorporate them into your environment. By the end of this Palo Alto Networks book, you will have mastered the skills needed to design and configure SASE-compliant remote connectivity and prevent credential theft with credential detection. What you will learnUnderstand how log forwarding is configured on the firewallFocus on effectively enabling remote accessExplore alternative ways for connecting users and remote networksProtect against phishing with credential detectionUnderstand how to troubleshoot complex issues confidentlyStrengthen the security posture of your firewallsWho this book is for This book is for anyone who wants to learn more about remote access for users and remote locations by using GlobalProtect and Prisma access and by deploying Large Scale VPN. Basic knowledge of Palo Alto Networks, network protocols, and network design will be helpful, which is why reading Mastering Palo Alto Networks is recommended first to help you make the most of this book.

The Only Official Google Cloud Study Guide The Official Google Cloud Certified Associate Cloud Engineer Study Guide, provides everything you need to prepare for this important exam and master the skills necessary to land that coveted Google Cloud Engineering certification. Beginning with a pre-book assessment quiz to evaluate what you know before you begin, each chapter features exam objectives and review questions, plus the online learning environment includes additional complete practice tests. Written by Dan Sullivan, a popular and experienced online course author for machine learning, big data, and Cloud topics, Official Google Cloud Certified Associate Cloud Engineer Study Guide is your ace in the hole for deploying and managing Google Cloud Services. • Select the right Google service from the various choices based on the application to be built • Compute with Cloud VMs and managing VMs • Plan and deploying storage • Network and configure access and security Google Cloud Platform is a leading public cloud that provides its users to many of the same software, hardware, and networking infrastructure used to power Google services. Businesses, organizations, and individuals can launch servers in minutes, store petabytes of data, and implement global virtual clouds with the Google Cloud Platform. Certified Associate Cloud Engineers have demonstrated the knowledge and skills needed to deploy and operate infrastructure, services, and networks in the Google Cloud. This exam guide is designed to help you understand the Google Cloud Platform in depth so that you can meet the needs of those operating resources in the Google Cloud.

Cortex XSOAR is the Security Orchestration, Automation and Response (SOAR) solution from Palo Alto Networks. Cortex XSOAR provides a centralized security orchestration and Automation solution to accelerate incident response and increase analyst productivity. A SOAR platform integrates your organization's security and monitoring tools, helping you centralize, standardize your incident handling processes.This book is a beginner friendly, step by step, practical guide that helps you to understand and learn Palo Alto Cortex XSOAR from scratch. No previous knowledge about the product is required and have explained all the important topics step by step, with screenshots.Covers,1) Solution architecture2) Incident lifecycle in Cortex XSOAR3) Integrations and incident creation4) Playbook development5) Layout customization6) Report creation7) Backup options8) Threat Intel management and EDL integration.9) Introduction to MSSP. Though Arista Networks is a relative newcomer in the data center and cloud networking markets, the company has already had considerable success. In this book, renowned consultant and technical author Gary Donahue (Network Warrior) provides an in-depth, objective guide to Arista's lineup of hardware, and explains why its network switches and Extensible Operating System (EOS) are so effective. Anyone with a CCNA or equivalent knowledge will benefit from this book, especially entrenched administrators, engineers, or architects tasked with building an Arista network. Is Arista right for your data center? Pick up this guide and find out. Topic highlights include: SysDB: the EOS system database that holds state, statuses, and variables Multichassis Link Aggregation (MLAG): for linking a port-channel to multiple switches instead of just one Latency Analyzer (LANZ): the interface-buffer troubleshooting tool with a reporting granularity of one millisecond VM Tracer: for adding, changing, and removing VLANs without human interaction Zero-Touch Provisioning (ZTP): for remote switch configuration Hardware advantages: including merchant silicon, low-latency networking, and power consumption Gotchas: issues with Arista switches or systems

Professional NoSQL

F5 Networks Application Delivery Fundamentals Study Guide

JUNOS High Availability

Exam Practice Questions For Palo Alto Networks (PCNSE6) Exam Prep LATEST VERSION

Formerly Notes and Reports in Computer Science and Applied Mathematics

VMware NSX Automation Fundamentals

Network World

A hands-on guide to leveraging NoSQL databases NoSQL databases are an efficient and powerful tool for storing and manipulating vast quantities of data. Most NoSQL databases scale well as data grows. In addition, they are often malleable and flexible enough to accommodate semi-structured and sparse data sets. This comprehensive hands-on guide presents fundamental concepts and practical solutions for getting you ready to use NoSQL databases. Expert author Shashank Tiwari begins with a helpful introduction on the subject of NoSQL, explains its characteristics and typical uses, and looks at where it fits in the application stack. Unique insights help you choose which NoSQL solutions are best for solving your specific data storage needs. Professional NoSQL: Demystifies the concepts that relate to NoSQL databases, including column-family oriented stores, key/value databases, and document databases. Delves into installing and configuring a number of NoSQL products and the Hadoop family of products. Explains ways of storing, accessing, and querying data in NoSQL databases through examples that use MongoDB, HBase, Cassandra, Redis, CouchDB, Google App Engine Datastore and more. Looks at architecture and internals. Provides guidelines for optimal usage, performance tuning, and scalable configurations. Presents a number of tools and utilities relating to NoSQL, distributed platforms, and scalable processing, including Hive, Pig, RRDtool, Nagios, and more.

Imagine what you could do if scalability wasn't a problem. With this hands-on guide, you'll learn how the Cassandra database management system handles hundreds of terabytes of data while remaining highly available across multiple data centers. This expanded second edition—updated for Cassandra 3.0—provides the technical details and practical examples you need to put this database to work in a production environment. Authors Jeff Carpenter and Eben Hewitt demonstrate the advantages of Cassandra's non-relational design, with special attention to data modeling. If you're a developer, DBA, or application architect looking to solve a database scaling issue or future-proof your application, this guide helps you harness Cassandra's speed and flexibility. Understand Cassandra's distributed and decentralized structure Use the Cassandra Query Language (CQL) and cqlsh—the CQL shell Create a working data model and compare it with an equivalent relational model Develop sample applications using client drivers for languages including Java, Python, and Node.js Explore cluster topology and learn how nodes exchange data Maintain a high level of performance in your cluster Deploy Cassandra on site, in the Cloud, or with Docker Integrate Cassandra with Spark, Hadoop, Elasticsearch, Solr, and Lucene

Here's the book you need to prepare for the JNCIA exam, JN0-201, from Juniper Networks. Written by a team of Juniper Network trainers and engineers, this Study Guide provides: Assessment testing to focus and direct your studies In-depth coverage of official test objectives Hundreds of challenging practice questions, in the book and on the CD Authoritative coverage of all test objectives, including: Working with the JUNOS software Implementing Juniper Networks boot devices Troubleshooting Routing Information Protocol Implementing a routing policy Configuring and monitoring an OSPF Network Implementing Border Gateway Protocol Monitoring and troubleshooting an IS-IS network Understanding the Reverse Path Forwarding process Operating firewall filters Using Multiprotocol Label Switching Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

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

JNCIA: Juniper Networks Certified Internet Associate Study Guide

The Definitive Classic in Adult Education and Human Resource Development

Microsoft Manual of Style

Exam JN0-201

Grace Hopper and the Invention of the Information Age

Navigating the Digital Age

A Computational Logic Handbook

Deploy and manage industry-leading PAN-OS 10.x solutions to secure your users and infrastructure Key FeaturesUnderstand how to optimally use PAN-OS featuresBuild firewall solutions to safeguard local, cloud, and mobile networksProtect your infrastructure and users by implementing robust threat prevention solutionsBook Description Palo Alto Networks' integrated platform makes it easy to manage network and cloud security along with endpoint protection and a wide range of security services. This book is an end-to-end guide to configure firewalls and deploy them in your network infrastructure. You will see how to quickly set up, configure and understand the technology, and troubleshoot any issues that may occur. This book will serve as your go-to reference for everything from setting up to troubleshooting complex issues. You will learn your way around the web interface and command-line structure, understand how the technology works so you can confidently predict the expected behavior, and successfully troubleshoot any anomalies you may encounter. Finally, you will see how to deploy firewalls in a cloud environment, and special or unique considerations when setting them to protect resources. By the end of this book, for your configuration setup you will instinctively know how to approach challenges, find the resources you need, and solve most issues efficiently. What you will learnExplore your way around the web interface and command lineDiscover the core technologies and see how to maximize your potential in your networkIdentify best practices and important considerations when configuring a security policyConnect to a freshly booted appliance or VM via a web interface or command-line interfaceGet your firewall up and running with a rudimentary but rigid configurationGain insight into encrypted sessions by setting up SSL decryptionTroubleshoot common issues, and deep-dive into flow analyticsConfigure the GlobalProtect VPN for remote workers as well as site-to-site VPNWho this book is for The book is for network and security professionals, and administrators who want to bring in the power of Palo Alto Networks and firewalls to secure their networks. Engineers should have a good grasp of networking and routing protocols, basic knowledge of stateful or next-generation firewalls is helpful but not required.

Welcome to the all-new second edition of Navigating the Digital Age. This edition brings together more than 50 leaders and visionaries from business, science, technology, government, academia, cybersecurity, and law enforcement. Each has contributed an exclusive chapter designed to make us think in depth about the ramifications of this digital world we are creating. Our purpose is to shed light on the vast possibilities that digital technologies present for us, with an emphasis on solving the existential challenge of cybersecurity. An important focus of the book is centered on doing business in the Digital Age—particularly around the need to foster a mutual understanding between technical and non-technical executives when it comes to the existential issues surrounding cybersecurity. This book has come together in three parts. In Part 1, we focus on the future of threat and risks. Part 2 emphasizes lessons from today's world, and Part 3 is designed to help you ensure you are covered today. Each part has its own flavor and personality, reflective of its goals and purpose. Part 1 is a bit more futuristic, Part 2 a bit more experiential, and Part 3 a bit more practical. How we work together, learn from our mistakes, deliver a secure and safe digital future—these are the elements that make up the core thinking behind this book. We cannot afford to be complacent. Whether you are a leader in business, government, or education, you should be knowledgeable, diligent, and action-oriented. It is our sincerest hope that this book provides answers, ideas, and inspiration. If we fail on the cybersecurity front, we put all of our hopes and aspirations at risk. So we start this book with a simple proposition: When it comes to cybersecurity, we must succeed.

The only study guide or material you'll need to prepare for the F5 Networks Application Delivery Fundamentals Exam. From the author of the most successful, popular and bestselling F5 technical books available today and the author of the first freely available study guide for this exam. The book's authors have taken great care to ensure all exam topics and fundamental networking areas are covered in full. The OSI Model, the Data Link, Network, Transport and Application Layers, Switching & Routing, F5 Solutions, Load Balancing, Security and Application Delivery Platforms are all covered in depth. No prior knowledge or experience is assumed. There are 13 chapters, 90 diagrams and over 70 test questions to ensure you have everything necessary to prepare for and pass the exam with confidence. Download of the PDF file has been disabled.

If you are new to Fortigate firewall, or just moving from another firewall platform (Check-Point, Palo alto), then this book is for you. here you will learn how to: Configure your administrator account with MFABackup revisionsConfigure Interfaces and servicesUnderstand Your Firewall SessionsAnalyze LogsManage your memory resourcesDiagnose With CLI commandsFortigate Firewall Admin Pocket Guide is here for one purpose only. to give you the skills to administrate your Fortigate firewall Fast with a solid foundationThis Book is For Beginners and Intermediate User

The Accidental Administrator

Cisco Router Step-By-Step Configuration Guide

Microsoft Azure Security Center

Palo Alto Cortex XSOAR

Introduction to FortiGate Part-1 Infrastructure

Software Defined Networks

Arista Warrior

Written and designed to assist students advance their literacy skills and vocabularies. Each unit covers an event that is of interest and significance to teenagers and young adults.

Maximize the impact and precision of your message! Now in its fourth edition, the Microsoft Manual of Style provides essential guidance to content creators, journalists, technical writers, editors, and everyone else who writes about computer technology. Direct from the Editorial Style Board at Microsoft—you get a comprehensive glossary of both general technology terms and those specific to Microsoft; clear, concise usage and style guidelines with helpful examples and alternatives; guidance on grammar, tone, and voice; and best practices for writing content for the web, optimizing for accessibility, and communicating to a worldwide audience. Fully updated and optimized for ease of use, the Microsoft Manual of Style is designed to help you communicate clearly, consistently, and accurately about technical topics—across a range of audiences and media.

Your easy-to-follow step-by-step guide to configuring a Cisco router from the ground up The Accidental Administrator: Cisco Router Step-by-Step Configuration Guide is packed with more than 30 easy-to-follow interactive exercises, loads of screen captures, and lots of step-by-step examples to help you build a working router from scratch. Easily the most straightforward approach to learning how to configure a Cisco router, this book is filled with practical tips and secrets learned from years of Don's teaching and consulting on Cisco network devices. As a bonus, you won't waste your time on boring theory. All the essentials are covered in chapters on installing, backups and restores, and TCP/IP. You'll learn the nitty-gritty on subnetting, remote administration, routing protocols, static routing, access-control lists, site-to-site VPNs, network address translation (NAT), DHCP, password recovery, and security. There's even an entire chapter on the new Internet Protocol version 6 (IPv6). Here's just some of what you'll find: How to configure and manage access lists How to set up a site-to-site VPN How to implement IPv6 All the information is presented in a straightforward style that you can understand and use right away. With The Accidental Administrator: Cisco Router Step-by-Step Configuration Guide you'll be able to sit down with your routers 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 'er done" in a minimal amount of time In addition, there are supporting videos and a supporting webpage to provide even more help and updated information.

Mastering Palo Alto NetworksBuild, configure, and deploy network solutions for your infrastructure using features of PAN-OSPackt Publishing Ltd

A Real-World Guide to Understanding Arista Switches and EOS

The Water Supply of Sussex

Mastering Windows Security and Hardening

The complete guide to planning, configuring, and managing Application Centric Infrastructure Information Rules

Penetration Testing Azure for Ethical Hackers

"For an engineer determined to refine and secure Internet operation or to explore alternative solutions to persistent problems, the insights provided by this book will be invaluable." —Vint Cerf, Internet pioneer TCP/IP Illustrated, Volume 1, Second Edition, is a detailed and visual guide to today's TCP/IP protocol suite. Fully updated for the newest innovations, it demonstrates each protocol in action through realistic examples from modern Linux, Windows, and Mac OS environments. There's no better way to discover why TCP/IP works as it does, how it reacts to common conditions, and how to apply it in your own applications and networks. Building on the late W. Richard Stevens' classic first edition, author Kevin R. Fall adds his cutting-edge experience as a leader in TCP/IP protocol research, updating the book to fully reflect the latest protocols and best practices. He first introduces TCP/IP's core goals and architectural concepts, showing how they can robustly connect diverse networks and support multiple services running concurrently. Next, he carefully explains Internet addressing in both IPv4 and IPv6 networks. Then, he walks through TCP/IP's structure and function from the bottom up: from link layer protocols—such as Ethernet and Wi-Fi—through network, transport, and application layers. Fall thoroughly introduces ARP, DHCP, NAT, firewalls, ICMPv4/ICMPv6, broadcasting, multicasting, UDP, DNS, and much more. He offers extensive coverage of reliable transport and TCP, including connection management, timeout, retransmission, interactive data flow, and congestion control. Finally, he introduces the basics of security and cryptography, and illuminates the crucial modern protocols for protecting security and privacy, including EAP, IPsec, TLS, DNSSEC, and DKIM. Whatever your TCP/IP experience, this book will help you gain a deeper, more intuitive understanding of the entire protocol suite so you can build better applications and run more reliable, efficient networks.

Looking to step into the Network Security field with the Fortigate firewall? Or are you required to manage a FortiGate NGFW for your organization? Then this is the right book for you! The FortiGate is an amazing device with many cybersecurity features to protect your network. If you are new to FortiGate's then this is the perfect book for you! This book will cover general overview of working with Fortinet. Also, you will gain a solid understanding on day to day administrative tasks. Next, you will learn how FortiGate interacts with various layer-2 protocol. Also you will get a chance how to filter network traffic and apply security policies which is very exciting. Lastly, you will learn about the session table and how Fortigate handles traffic. Below is a full list of what this book covers: Chapter One - Introduction to FortiGate-Identify platform features of FortiGate-Describe Security Processor Unit SPU-Identify factory defaults-Understand the different operational modes-Understand FortiGate and FortiGuard Relationship-Manage administrator profiles-Manage administrative profiles-Manage network interfaces-Manage basic services-backup and restore config file-update and downgrade firmware-Understand CLI structure-Understand GUI navigation-Initial configurationChapter - 2 - Layer two technologies-Configuration of layer-2 VLANs-Describe VLANs and VLAN tagging process-Describe FortiOS Transparent Mode-Configure FortiOS Transparent Mode settings-Describe Transparent Mode Bridge Table-Describe MAC forwarding-Describe how to find MAC address on FortiOS-Describe Forwarding Domains-Describe and configure Virtual Switches-Describe Spanning Tree Protocol-Describe and Configure various NAT Mode layer-2 protocols-Describe and configure Layer-3 VLAN interface-Describe Virtual Wire Pairing-Describe and Configure VXLANChapter-3 Layer Three Technologies: -Configuration of Static Routes-implementation of Policy-Based Routes-Control traffic for well-known Internet Services-Interpret the FortiOS Routing Table-Understand FortiOS anti-spoofing mechanism-Implement route failover and floating route-Understand ECMP-Recognize active route vs standby route vs inactive routes-Use built in sniffer and diagnose flow debug tools, -Understand Session Table Entry.Chapter 4 - Firewall Policy and NAT-Identify components in Firewall Policy-Describe how traffic matches Firewall Policy Entries-Configure Firewall Policy Logging-Describe Policy GUI list views-Describe Policy ID's vs Policy Sequence numbers-Described where objects are referenced-Explain Name restrictions on Firewall Policies-Perform Firewall Policy re-ordering-Describe NAT and PAT-Explain different configuration modes for NAT-Configure and Describe SNAT and DNAT VIPs-Troubleshoot NAT issues

Simulate real-world attacks using tactics, techniques, and procedures that adversaries use during cloud breaches Key FeaturesUnderstand the different Azure attack techniques and methodologies used by hackersFind out how you can ensure end-to-end cybersecurity in the Azure ecosystemDiscover various tools and techniques to perform successful penetration tests on your Azure infrastructureBook Description "If you're looking for this book, you need it." — 5* Amazon Review Curious about how safe Azure really is? Put your knowledge to work with this practical guide to penetration testing. This book offers a no-faff, hands-on approach to exploring Azure penetration testing methodologies, which will get up and running in no time with the help of real-world examples, scripts, and ready-to-use source code. As you learn about the Microsoft Azure platform and understand how hackers can attack resources hosted in the Azure cloud, you'll find out how to protect your environment by identifying vulnerabilities,

along with extending your pentesting tools and capabilities. First, you'll be taken through the prerequisites for pentesting Azure and shown how to set up a pentesting lab. You'll then simulate attacks on Azure assets such as web applications and virtual machines from anonymous and authenticated perspectives. In the later chapters, you'll learn about the opportunities for privilege escalation in Azure tenants and ways in which an attacker can create persistent access to an environment. By the end of this book, you'll be able to leverage your ethical hacking skills to identify and implement different tools and techniques to perform successful penetration tests on your own Azure infrastructure. What you will learn

Identify how administrators misconfigure Azure services, leaving them open to exploitation

Understand how to detect cloud infrastructure, service, and application misconfigurations

Explore processes and techniques for exploiting common Azure security issues

Use on-premises networks to pivot and escalate access within Azure

Diagnose gaps and weaknesses in Azure security implementations

Understand how attackers can escalate privileges in Azure AD

Who this book is for

This book is for new and experienced infosec enthusiasts who want to learn how to simulate real-world Azure attacks using tactics, techniques, and procedures (TTPs) that adversaries use in cloud breaches. Any technology professional working with the Azure platform (including Azure administrators, developers, and DevOps engineers) interested in learning how attackers exploit vulnerabilities in Azure hosted infrastructure, applications, and services will find this book useful.

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, usernames, 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!

The Complete Cisco VPN Configuration Guide

Palo Alto Networks Certified Network Security Engineer 6 (PCNSE6) Exam Practice Questions & Dumps

A Practical Guide for Librarians

Learning PowerCLI

A Strategic Guide to the Network Economy

Build, configure, and deploy network solutions for your infrastructure using features of PAN-OS

Fortigate Firewall Admin Pocket Guide

With increased use of Internet connectivity and less reliance on private WAN networks, virtual private networks (VPNs) provide a much-needed secure method of transferring critical information. As Cisco Systems integrates security and access features into routers, firewalls, clients, and concentrators, its solutions become ever more accessible to companies with networks of all sizes. The Complete Cisco VPN Configuration Guide contains detailed explanations of all Cisco VPN products, describing how to set up IPsec and Secure Sockets Layer (SSL) connections on any type of Cisco device, including concentrators, clients, routers, or Cisco PIX and Cisco ASA security appliances. With copious configuration examples and troubleshooting scenarios, it offers clear information on VPN implementation designs.

- A complete resource for understanding VPN components and VPN design issues
- Learn how to employ state-of-the-art VPN connection types and implement complex VPN configurations on Cisco devices, including routers, Cisco PIX and Cisco ASA security appliances, concentrators, and remote access clients
- Discover troubleshooting tips and techniques from real-world scenarios based on the author's vast field experience
- Filled with relevant configurations you can use immediately in your own network

Securing Remote Access in Palo Alto Networks

Mastering Palo Alto Networks

Literacy in Events

Deploy and Manage Industry-Leading PAN-OS Solutions to Secure Your Users and Infrastructure