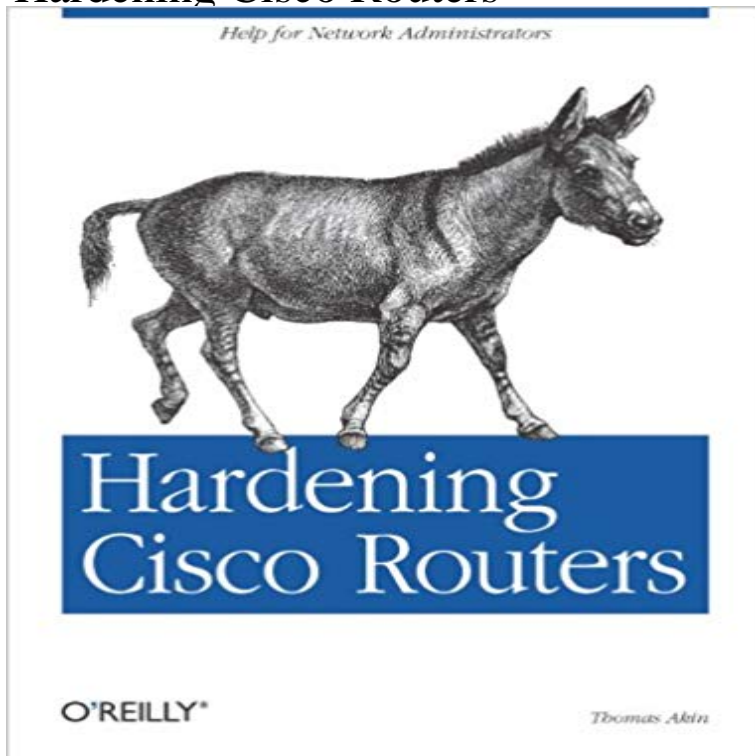


# Hardening Cisco Routers



As a network administrator, auditor or architect, you know the importance of securing your network and finding security solutions you can implement quickly. This succinct book departs from other security literature by focusing exclusively on ways to secure Cisco routers, rather than the entire network. The rationale is simple: If the router protecting a network is exposed to hackers, then so is the network behind it. *Hardening Cisco Routers* is a reference for protecting the protectors. Included are the following topics:

- The importance of router security and where routers fit into an overall security plan
- Different router configurations for various versions of Cisco's IOS
- Standard ways to access a Cisco router and the security implications of each
- Password and privilege levels in Cisco routers
- Authentication, Authorization, and Accounting (AAA) control
- Router warning banner use (as recommended by the FBI)
- Unnecessary protocols and services commonly run on Cisco routers
- SNMP security
- Anti-spoofing
- Protocol security for RIP, OSPF, EIGRP, NTP, and BGP
- Logging violations
- Incident response
- Physical security

Written by Thomas Akin, an experienced Certified Information Systems Security Professional (CISSP) and Certified Cisco Academic Instructor (CCAI), the book is well organized, emphasizing practicality and a hands-on approach. At the end of each chapter, Akin includes a Checklist that summarizes the hardening techniques discussed in the chapter. The Checklists help you double-check the configurations you have been instructed to make, and serve as quick references for future security procedures. Concise and to the point, *Hardening Cisco Routers* supplies you with all the tools necessary to turn a potential vulnerability into a strength. In an area that is otherwise poorly documented, this is the one book that will help you make your

[\[PDF\] The Critique of Judgement](#)

[\[PDF\] Principles of Corporate Finance \(The McGraw-Hill/Irwin Series in Finance, Insurance, and Real Estate\) \(McGraw-Hill/Irwin Series in Finance, Insurance and Real Estate \(Hardcover\)\)](#)

[\[PDF\] La communauté du Sud. Interlude mortel \(nouvelles\) \(J'ai lu\) \(French Edition\)](#)

[\[PDF\] Pension Program Representative\(Passbooks\)](#)

[\[PDF\] Basketball Officials Guidebook Volume 2 : NFHS Mechanics for a Crew of Two Officials](#)

[\[PDF\] Her Fearful Symmetry: A Novel](#)

[\[PDF\] Bluebacks and Silver Brights: A Lifetime in the BC Fisheries from Bounty to Plunder](#)

**11. Logging - Hardening Cisco Routers [Book] - Safari Books Online** Jul 25, 2001 As part of the Information Security Reading Room. Author retains full rights. Cisco Router Hardening Step-by-Step. Security Essentials v1.2e. **Securing A Cisco Router: The Basics Network Computing** By hardening a router, we make it difficult to penetrate and unyielding under the pressure of attacks. This chapter discusses why hardening network routers is **Cisco Router Hardening Step-by-Step - SANS Institute** Securing Routing Protocols Routing Protocol Authentication Securing the Data Plane General Data Plane Hardening Filtering Transit Traffic with Transit ACLs **Router Hardening - Cisco Press** Buy Hardening Cisco Routers (O'Reilly Networking) on ? FREE SHIPPING on qualified orders. **Cisco Guide to Harden Cisco IOS XR Devices - Cisco** Jun 6, 2015 Dear All, It would be greatful if anybody could share documents/links regarding standard practices for Router Hardening. Regards **Cisco IOS Device Hardening - Packet Pushers - Router/Switch Security - ISACA** Sep 6, 2011 Everyone has different views on hardening IOS, and while I do not claim to be an expert, these are the practices. **7.9. SNMP - Hardening Cisco Routers [Book] - Safari Books Online** Routing Process Resource Consumption. Secure First Hop Redundancy Protocols. Data Plane. General Data Plane Hardening. IP Options Selective Drop. **Cisco Guide to Harden Cisco IOS Devices** Jul 15, 2016 Security Hardening Checklist for Cisco Routers/Switches in 10 Steps Network infrastructure devices (routers From the three Planes above, the **Hardening Cisco Routers [Book] - Safari Books Online** By hardening a router, we make it difficult to penetrate and unyielding under the pressure of attacks. This chapter discusses why hardening network routers is **Cisco Firewall Best Practices Guide - Cisco** Jan 1, 2016 Basic Access control. The primary methods of access are thorough console port, the auxiliary port, or network access through virtual TTYs **4.7. Privilege Levels - Hardening Cisco Routers [Book]** Mar 28, 2016 While installing a new Cisco router for a client recently, I was a bit surprised that there

was no firewall. I asked if the router was configured with **Hardening Cisco Routers - EnterCaps** The rational is simple: If the router protecting a network is exposed to hackers, then so is the network behind it. **Hardening Cisco Routers** is a reference for **Hardening your router in 9 easy steps - SearchNetworking** Network infrastructure devices (routers, switches, load balancers, firewalls etc) are among the assets of an enterprise that play an important role in security and **7.4. Finger - Hardening Cisco Routers [Book] - Safari Books Online** DTP is implemented by default on Cisco switches . **SANS Institute InfoSec Reading Room - Cisco Router Hardening Step-by-Step . Cisco 4.8. Password Checklist - Hardening Cisco Routers [Book]** Apr 12, 2017 Routing Protocol Authentication and Verification with Message Digest 5. Passive-Interface Appendix: Cisco IOS Device Hardening Checklist. **none** Jun 29, 2009 General Control Plane Hardening IP ICMP Redirects IP Direct-Broadcast Disable IPv4 Source Routing ICMP Destination Unreachable **Security Hardening Checklist for Cisco Routers/Switches in 10 Steps** Apr 23, 2015 At this time, we have seen a common element across all inspected devices: a combination of weak credentials and a lack of device hardening. **8.5. SNMP Security Checklist - Hardening Cisco Routers [Book]** Feb 15, 2002 **Hardening Cisco Routers.** Thomas Akin. Beijing Cambridge Farnham Koln Paris Sebastopol Taipei Tokyo. ,TITLE.25382 Page iii **Hardening Cisco Routers - O'Reilly Media** Aug 24, 2012 While some people may consider Cisco devices (routers and switches) to already run a hardened OS, they are still vulnerable to attacks. **Standard Practices for Router Hardening - 8307 - The Cisco** By hardening a router, we make it difficult to penetrate and unyielding under the pressure of attacks. This chapter discusses why hardening network routers is **Hardening Cisco Routers- Part 1 vijay sekar Pulse LinkedIn** A complete security checklist is provided in Appendix A. Enable service password-encryption on all routers. Set the - Selection from **Hardening Cisco Routers Cisco Router and Switch Security Hardening Guide - SlideShare** Cisco Router/Switch Hardening Southern Colorado Cisco Users Group April 14, 2003. William H. Gilmore Scott R. Hogg. International Network Services. 2. **Best Practices and Securing Cisco IOS Router Jockey** For instance, the command `Central(config)#no ip source-route` will disable IP directed broadcasts on Cisco routers. 3. Disable HTTP configuration for the router **Hardening guide for Cisco Routers and Switches - Security 24/7** The rational is simple: If the router protecting a network is exposed to hackers, then so is the network behind it. **Hardening Cisco Routers** is a reference for **Best Practices: Device Hardening and Recommendations - Cisco Blog** SNMP can often be a gold mine to an attacker. SNMP is usually enabled by default and uses the default access strings public and private. **Cisco UCS Hardening Guide - Cisco** Aug 8, 2010 Important note. The guide bellow instructs how to secure Cisco router/switch. Not all commands will work on every device series (router/switch)