



Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.1(3)N1(1)

First Published: December 05, 2011

Last Modified: December 28, 2011

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25845-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface xv

Audience xv

Document Conventions xv

Documentation Feedback xvi

Obtaining Documentation and Submitting a Service Request xvii

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview 5

Authentication, Authorization, and Accounting 5

RADIUS and TACACS+ Security Protocols 6

SSH and Telnet 6

IP ACLs 7

CHAPTER 3

Configuring Authentication, Authorization, and Accounting 9

Information About AAA 9

AAA Security Services 9

Benefits of Using AAA 10

Remote AAA Services 10

AAA Server Groups 10

AAA Service Configuration Options 11

Authentication and Authorization Process for User Logins 12

Prerequisites for Remote AAA 13

Guidelines and Limitations for AAA 14

Configuring AAA 14

Configuring Console Login Authentication Methods 14

Configuring Default Login Authentication Methods	15
Enabling Login Authentication Failure Messages	16
Configuring AAA Command Authorization	17
Enabling MSCHAP Authentication	19
Configuring AAA Accounting Default Methods	20
Using AAA Server VSAs	21
VSAs	21
VSA Format	22
Specifying Switch User Roles and SNMPv3 Parameters on AAA Servers	22
Monitoring and Clearing the Local AAA Accounting Log	23
Verifying the AAA Configuration	23
Configuration Examples for AAA	24
Default AAA Settings	24
<hr/>	
CHAPTER 4	Configuring RADIUS 25
Configuring RADIUS	25
Information About RADIUS	25
RADIUS Network Environments	25
Information About RADIUS Operations	26
RADIUS Server Monitoring	26
Vendor-Specific Attributes	27
Prerequisites for RADIUS	28
Guidelines and Limitations for RADIUS	28
Configuring RADIUS Servers	28
Configuring RADIUS Server Hosts	29
Configuring RADIUS Global Preshared Keys	30
Configuring RADIUS Server Preshared Keys	31
Configuring RADIUS Server Groups	32
Configuring the Global Source Interface for RADIUS Server Groups	33
Allowing Users to Specify a RADIUS Server at Login	34
Configuring the Global RADIUS Transmission Retry Count and Timeout Interval	35
Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server	36
Configuring Accounting and Authentication Attributes for RADIUS Servers	37
Configuring Periodic RADIUS Server Monitoring	38

- Configuring the Dead-Time Interval 39
- Manually Monitoring RADIUS Servers or Groups 40
- Verifying the RADIUS Configuration 41
- Displaying RADIUS Server Statistics 41
- Clearing RADIUS Server Statistics 41
- Configuration Examples for RADIUS 42
- Default Settings for RADIUS 42

CHAPTER 5**Configuring TACACS+ 45**

- About Configuring TACACS+ 45
- Information About Configuring TACACS+ 45
 - TACACS+ Advantages 45
 - User Login with TACACS+ 46
 - Default TACACS+ Server Encryption Type and Preshared Key 46
 - Command Authorization Support for TACACS+ Servers 47
 - TACACS+ Server Monitoring 47
- Prerequisites for TACACS+ 47
- Guidelines and Limitations for TACACS+ 48
- Configuring TACACS+ 48
 - TACACS+ Server Configuration Process 48
 - Enabling TACACS+ 49
 - Configuring TACACS+ Server Hosts 49
 - Configuring TACACS+ Global Preshared Keys 50
 - Configuring TACACS+ Server Preshared Keys 51
 - Configuring TACACS+ Server Groups 52
 - Configuring the Global Source Interface for TACACS+ Server Groups 54
 - Specifying a TACACS+ Server at Login 55
 - Configuring AAA Authorization on TACACS+ Servers 55
 - Configuring Command Authorization on TACACS+ Servers 57
 - Testing Command Authorization on TACACS+ Servers 58
 - Enabling and Disabling Command Authorization Verification 59
 - Configuring Privilege Level Support for Authorization on TACACS+ Servers 59
 - Permitting or Denying Commands for Users of Privilege Roles 61
 - Configuring the Global TACACS+ Timeout Interval 63
 - Configuring the Timeout Interval for a Server 63

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.