



Study Guide for the 2006 Cisco CCIE[®] Security Written Exam

Farrukh Haroon
Colby LeMaire, CCIE#12968
Brad Ellis, CCIE#5796

Network Learning
www.ccbootcamp.com

NLI's Study Guide for the Cisco CCIE Security Written Exam

Authors: Colby LeMaire, Farrukh Haroon, and Brad Ellis

Copyright© 2006 Network Learning, Inc.

Published by:

Network Learning Inc (Cisco Learning Partner)

1997 Whitney Mesa Dr

Henderson, NV 89014 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First printing August 2006 ISBN: 1-931881-17-0

UPC: 82251881170

Warning and Disclaimer

This book is designed to provide information the Cisco Security written exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, editors, and Network Learning Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Network Learning Inc.

Trademark Acknowledgements

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Network Learning Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Network Learning Inc, our goal is to create advanced technical material of the highest quality and value. Each book is authored with attention to detail, undergoing strenuous development that involves input from a variety of technical experts.

For technical support on this book, please visit: www.securityie.com

Readers' feedback is a natural part of this process. If you have any comments regarding how we could improve the quality of our materials, or otherwise change it to better suit your needs, you can contact us through e-mail at sales@ccbootcamp.com. Please make sure to include the book title and ISBN number in your message. Also, feel free to visit our website: www.ccbootcamp.com for information on many more great products!

Thank you for your input

About the contributors:

Author – Colby LeMaire

Colby LeMaire (CCIE #12968, CISSP, CCDP, CCNP, MCSE, MCDBA) is a Network Consulting Engineer with Cisco Systems. He has over 12 years of experience in networking and security with most of that time spent with the Department of Defense and other Government agencies. He holds a BS degree in Computer Information Systems and has most recently focused on Network Management and Security projects.

Author – Farrukh Haroon

Farrukh Haroon (CCDA, CCSP, CARLSS, CSEP) is a network engineer currently employed with a Cisco Systems Silver Partner in the Middle East. Farrukh is currently focussing on network security and is preparing for his CCIE Security Lab Exam.

Author – Brad Ellis

Brad Ellis (CCIE #5796, CCSI #30482, CSS1, CCDP, CCNP, MCNE, MCSE) works as a network engineer and is CEO of Network Learning Inc. He has been dedicated to the networking industry for over 12 years. Brad has worked on large scale security assessments and infrastructure projects. He is currently focusing his efforts in the security and voice fields. Brad is a dual CCIE (R&S / Security) #5796.

(this page intentionally left blank)

Table of Contents

Chapter 1 Security Protocols	1
Authentication, Authorization and Accounting	1
AAA Overview	1
Overview: AAA Security Services	1
AAA Terminology	3
Benefits of Using AAA	3
AAA Configuration Process – Overview	4
AAA Request for Comments (RFCs).....	4
Remote Authentication Dial-In User Service (RADIUS).....	4
Introduction	4
Background Information.....	4
Authentication and Authorization	5
Accounting	6
Radius Packet Format	7
Radius Packet Types	7
Radius Files.....	8
Radius Attributes	9
No	10
IETF Attributes vs. VSAs	22
RADIUS Configuration Task List.....	23
AAA and RADIUS IOS Configuration	24
Named Method Lists for Authorization	25
Terminal Access Controller Access Control System Plus (TACACS+).....	26
Introduction	26
TACACS+ Packet Format	26
TACACS+ Encryption	28
TACACS+ Authentication	28
TACACS+ Authentication Example Sequence	29
TACACS+ Authorization.....	29
Attribute	37
RADIUS and TACACS+ Compared	41
Cryptographic Algorithms	41
Introduction	41
Symmetric Algorithms	42

Table of Contents (Continued)

Asymmetric Algorithms	43
Hash Functions	44
Digital Signatures.....	44
Advanced Encryption Standard (AES).....	44
Data Encryption Standard (DES)	46
Triple DES (3DES).....	46
Wireless Security Protocols	46
Introduction	46
Extensible Authentication Protocol (EAP)	47
Protected Extensible Authentication Protocol (PEAP).....	48
Temporal Key Integrity Protocol (TKIP)	48
802.11i.....	48
VPN Protocols	49
Introduction	49
Virtual Private Networks Defined	49
Virtual Private Networks Goals	50
Types of Virtual Private Networks	51
Benefits of Virtual Private Networks	54
VPN Security Protocols – IPSEC.....	54
IPSec Standards and Protocols	55
IPSec Terminology	56
IPSec Functionality	58
IPSec Modes and Packet Encapsulation.....	59
Encapsulating Security Payload (ESP)	59
Authentication Header (AH)	60
Authentication Header vs. ESP	62
Further Reading	63
VPN Security Protocols – Internet Key Exchange (IKE)	63
IKE Benefits	63
IKE Protocols.....	64
IKE Phases.....	64
IKE Main Mode and Aggressive Mode	65
IKE Authentication	66
Creating IKE Policies.....	67
Diffie Hellman.....	67
IPSEC and Fragmentation.....	69
IPSEC and GRE	69
IPSEC and QoS	71
Point to Point Tunneling Protocol	72

Table of Contents (Continued)

Configuration Summary: PPTP	73
Configuration Sample: Basic PAC Setup:.....	73
Layer 2 Tunneling Protocol	74
L2TP Benefits	75
L2TP Implementation Topologies	76
L2TP Security	76
Chapter 1 Questions	77
Chapter 1 Answers	89
Chapter 2 Application Protocols.....	91
Domain Name System (DNS)	91
Trivial File Transfer Protocol (TFTP).....	93
File Transfer Protocol (FTP).....	95
Hypertext Transfer Protocol (HTTP).....	96
Secure Socket Layer (SSL)	99
Simple Mail Transfer Protocol (SMTP)	100
Network Time Protocol (NTP)	103
Secure Shell (SSH).....	105
Simple Network Management Protocol (SNMP)	108
Lightweight Directory Access Protocol (LDAP)	110
Active Directory	111
Remote Data Exchange Protocol (RDEP)	111
Chapter 2 Questions	112
Chapter 2 Answers	117
Chapter 3 General Networking	118
Networking Basics / OSI Model.....	118
TCP/IP Model	119
Routing and Switching Concepts.....	120
Cisco Hierarchical Internetworking Model	120
Distance-Vector Routing Protocols	121
Link-State Routing Protocols	122
Hybrid Routing Protocols	122
Routing Loops.....	123
Route Summarization	123
Tunnels	126
Networking Standards.....	126
Protocol Mechanisms	128

Table of Contents (Continued)

Transmission Control Protocol (TCP)	129
User Datagram Protocol (UDP)	130
Address Resolution Protocol (ARP)	131
General Bridging Rules.....	133
LAN Switching	134
Routing Information Protocol (RIP) & RIP V2	134
Interior Gateway Routing Protocol (IGRP)	136
Open Shortest Path First (OSPF)	137
Enhanced Interior Gateway Routing Protocol (EIGRP)	147
Border Gateway Protocol (BGP).....	158
High-Level Data Link Control (HDLC)	169
Point-to-Point Protocol (PPP).....	169
Modems and Async.....	170
IP Multicast	170
Benefits of IP Multicast	171
IGMP and CGMP Multicast Protocols	172
IGMP Versions 1, 2, and 3	173
Wireless Standards.....	176
Wireless/802.11b	176
Wireless Networking Terms	177
802.1x Authentication.....	178
802.11 On Its Own is Inherently Insecure.....	179
Wireless Networks Are Targets for Intruders	180
802.11 Wired Equivalent Privacy (WEP).....	182
IPsec in a WLAN Environment	183
802.1x/EAP.....	183
EAP Authentication Protocols	186
EAP Authentication Summary.....	191
Chapter 2 Answers	199
Chapter 4 Security Technologies	201
Firewalls and Access Control	201
Introduction	201
Choosing the Right Firewall	201
Types of Firewalls	202
Anti-Virus and Anti-Spyware Solutions	207
Anti-Virus Software	207
Anti-Spyware Software	208

Table of Contents (Continued)

Content Filtering	208
Introduction	208
Network Address Translation.....	210
Introduction	210
Benefits	210
Terminology	211
Example 1 – Inside Local and Inside Global Addresses.....	212
Example 2 – Outside Local and Outside Global Addresses.....	213
Example 3 – Translation of all four addresses (two local and two global).....	214
More NAT Terminology.....	216
Summary of NAT Commands	216
NAT Order of Operation.....	217
Configuring IPSec-Based VPNs (Pre-Shared Keys).....	218
Configuring Scalable IPSec-Based VPNs Using Digital Certificates	229
What are Digital Certificates?	229
Introduction to Certificate Authorities (CA).....	229
Certificate Authority Support on Cisco Routers.....	230
Implementing IPSEC without CA Support.....	231
Implementing IPSEC with CA Support	231
Implementing IPSEC with Multiple Root CAs.....	232
How CA Certificates are used by IPSec Devices?	233
Registration Authorities.....	233
CA Configuration Steps on Cisco Routers	233
Verifying Keys and Certificates	239
CA Configuration Example	240
Configuring NAT & IPSec Together.....	243
Configuration for Router 3640-2b	243
Configuration for Router 3640-2b	245
Intrusion Detection and Prevention	247
Introduction	247
What is Intrusion Detection?	248
Intrusion Detection Terminology.....	248
Attack Identification and Analysis	249
IDS placement.....	251
Network-Based Intrusion Detection Systems (NIDS)	251
Host-Based Intrusion Detection Systems (HIDS).....	252
Intrusion Detection – Response Techniques and Corrective Actions.....	253
Intrusion Detection – Evasion Techniques	254
Cisco Threat Response (CTR)	256

Table of Contents (Continued)

Network-Based Application Recognition	263
Identity Technologies.....	264
Introduction	264
Authentication Factors	264
Some Identity Technologies.....	264
Chapter 4 Questions	270
Chapter 4 Questions.....	270
Chapter 4 Answers	287
Chapter 5 Security Applications.....	289
Cisco Secure ACS.....	289
Introduction	289
Benefits	289
Cisco Secure ACS for Windows Architecture	290
ACS Version 3.3.....	292
ACS Version 4.0.....	294
Features and Benefits of version 4.0	295
Installing Cisco Secure ACS	297
Administration of Cisco Secure ACS	299
Positioning ACS in your Network.....	301
Cisco Secure PIX Firewall	307
Introduction	307
Stateful Inspection Firewall Features.....	307
MANAGEMENT	311
Two Key Components of Cisco PIX Firewalls	313
Features of PIX Software Version 6.3	316
Cisco PIX Appliance Models.....	320
PIX Firewall Licensing	324
Adaptive Security Appliance Series	326
Cisco Adaptive Security Device Manager.....	329
Configuring NAT and PAT	331
Saving Your Configuration	333
Configuration Examples - Two Interfaces without NAT or PAT	334
Two Interfaces with NAT and PAT	337
Site-to-Site VPN Configuration	338
Configuring Overlapping Networks.....	341
Syslog Messages.....	343
Cisco IOS Firewall	346

Table of Contents (Continued)

Cisco IOS Firewall Features.....	347
Authentication Proxy.....	348
Introduction	348
Working.....	348
Authentication Proxy Screens.....	349
Compatibility	351
Configuring Authentication Proxy.....	351
Cisco IOS Firewall TCP Intercept.....	355
Modes	355
Configuration Sample	356
Cisco Context-Based Access Control (CBAC).....	356
Introduction	356
Traffic Filtering	356
Traffic Inspection and DoS Attack Protection	357
Limitations of CBAC.....	357
CBAC - Working	358
CBAC Deployment Scenarios.....	359
The CBAC Process	360
CBAC - Supported Protocols.....	361
CBAC - Limitations	362
Configuring CBAC.....	362
Cisco Secure Intrusion Detection System.....	370
Introduction	370
IDS/IPS Software.....	371
Cisco Intrusion Detection Sensors - Models	377
Cisco Intrusion Detection Solution for Routers and Switches.....	380
Cisco IDS / IPS Network Interfaces.....	380
Cisco Intrusion Detection Signatures.....	381
Signature Categories	381
Signature Engines	383
Cisco IDS Alarm Levels	384
Tuning IDS Signatures	384
Cisco Intrusion Detection Management.....	385
Cisco Intrusion Detection Event Monitoring	387
Cisco IDS Management and Monitoring – Ports and Protocols.....	389
Cisco IOS IDS – Configuration.....	390
Cisco VPN 3000 Series Concentrators.....	394
Introduction	394
Concentrators.....	394

Table of Contents (Continued)

Management	396
New Features in Version 4.7 (software)	396
Cisco VPN Concentrator Deployment Scenarios.....	397
VPN Clients	397
Cisco Catalyst Service Modules.....	400
Benefits	401
Firewall Services Module (FWSM)	402
Intrusion Detection System Service Module (IDSM).....	403
IPSEC VPN Services Module (VPNSM).....	404
SSL Services Module (SSLSM).....	405
MARS - Security Information Monitoring System.....	406
Introduction	406
Benefits	407
Appliances	408
Cisco VMS – Security Management System.....	408
Introduction	408
Application	408
Current Status.....	409
Cisco Router and Security Device Manager (SDM).....	409
SDM enabling a IOS Router	413
Chapter 5 Questions.....	414
Chapter 5 Answers	430
Chapter 6 Security General	432
Security Policy Best Practices.....	432
Standards Bodies and Security Organizations	435
Vulnerabilities.....	440
Know Your Enemy	441
Hacking Methodology.....	443
Common Attacks.....	444
Countermeasures	450
Chapter 6 Questions.....	454
Chapter 6 Answers	460
Chapter 7 Cisco General	461
Access Control Lists (ACLs).....	461
Logging	469
Show and Debug Commands	473

Table of Contents (Continued)

Controlling Access to a Cisco Router.....	483
Password Recovery.....	487
Encrypting Cisco Passwords	490
Disable Unnecessary Services	491
Layer-2 Switching Security Features	492
Chapter 7 Questions	499
Chapter 7 Answers	508