CCNA Security 210-260 Official Cert Guide
First Edition

ISBN-10: 1-58720-566-1
ISBN-13: 978-1-58720-566-8

Warning and Disclaimer

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 provided is on an "as is" basis. The author and the publisher 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 CD or programs accompanying it.

When reviewing corrections, always check the print number of your book. Corrections are made to printed books with each subsequent printing.

First Printing: June 2015

Corrections for July 20, 2017

Pg	Error - Sixth Printing	Correction
106	Chapter 5, First Bullet, Fourth Sentence Reads: This is the primary protocol used for this purpose, compared to OSCP and AAA.	Should read: This is the primary protocol used for this purpose, compared to OCSP and AAA.

Corrections for November 21, 2016

Pg	Error - Fifth Printing	Correction
252	Chapter 9, Example 9-11, Third to the Last Configuration Reads: **sw2# show llpd**	Should read: **sw2# show lldp**

Corrections for October 5, 2016

Pg	Error - Fourth Printing	Correction
133	Chapter 6, Figure 6-8, Configure IKE Policy Reads: Priority 1	Should read: Priority 2
133	Chapter 6, Figure 6-9, Second Row, Under Priority Reads: 1	Should read: 2
207	Chapter 8, Table 8-3, SSL Column, Second Row Reads: Starts with a secured channel and continues directly to security negations on a dedicated port.	Should read: Starts with a secured channel and continues directly to security negotiations on a dedicated port.
508	Chapter 20, Using the Exam Engine, Second Bullet Point, Last Sentence Reads: These timed exams not only allow you to	Should read: These timed exams not only allow you to study for the actual 210-260 IINS exam, they help you simulate the

	study for the actual 640-554 IINS exam, they help you simulate the time pressure that can occur on the actual exam.	time pressure that can occur on the actual exam.

Corrections for August 25, 2016

Pg	Error - Fourth Printing	Correction
24	Chapter 8, Example 8-2, Eight Command Reads: **ip local pool anyconnectPool 10.4.4.1-10.0.0.100 mask 255.255.255.0**	Should read: **ip local pool anyconnectPool 10.4.4.1-10.4.4.100 mask 255.255.255.0**

Corrections for August 11, 2016

Pg	Error - Fourth Printing	Correction
512	Appendix A, Chapter 5, Answer to Question 13 Reads: **13.** B and D	Should read: **13.** A, B and D

Corrections for May 13, 2016

Pg	Error - Third Printing	Correction
79	Chapter 4, Figure 4-3, Second Row of Boxes, Last Box. First Cloud Reads: WPLS WAN	Should read: MPLS WAN

Corrections for March 25, 2016

Pg	Error - Third Printing	Correction
122	Chapter 6, Figure 6-1, R1 public IP Reads: 28.0.0.1	Should read: 23.0.0.1

Corrections for March 20, 2016

Pg	Error - Third Printing	Correction
308	Chapter 11, Example 11-11, Sixth Line Reads: ! If we add time stamps to the syslog messages, those time stamps can assist it	Should read: ! If we add time stamps to the syslog messages, those time stamps can assist in
308	Chapter 11, Last Paragraph, First Sentence Reads: To configure logging, you just tell CCP what the IP address of your syslog server is and which level of logging you want to do to that IP address.	Should read: To configure logging, tell the CCP the address of your syslog server and what logging level you want to use.
310	Chapter 11, First Paragraph after Table 11-5, First Sentence Reads: An SNMP manager can send information to, receive request information from, or receive unsolicited information (called a trap) from a managed device (a router).	Should read: An SNMP manager can send information to, receive requested information from, or receive unsolicited information (called a trap) from a managed device (a router).

324	Chapter 12, Table 12-2, Fourth Row, IPv6 Reads: IPsec support is supposed to be "required." This really means that it is supported for IPv6 from the beginning, but IPv6 does not require it to be configured for IPv6 to work.	Should read: IPsec is fully supported in IPv6. In fact, IPsec was supposed to be mandatory when using IPv6, however IPv6 does not actually require IPsec to be enabled for IPv6 to work.
324	Chapter 12, Table 12-2, Fifth Row, IPv4 Reads: Multiple pieces in an IPv4 header.	Should read: An IPv4 header consists of multiple fields.
332	Chapter 12, Last Bullet, First Sentence Reads: ▪ **Mitigating DoS attacks**: *Denial of service* refers to willful attempts to disrupt legitimate users from getting access to the resources they intend to.	Should read: ▪ **Mitigating DoS attacks**: *Denial of service* refers to willful attempts to disrupt legitimate users from getting access to the resources they intend to use.
334	Chapter 12, The Focus on IPv6 Security, Second Sentence Reads: If an attacker issues a ping sweep of your network, he will not likely find all the devices via a traditional ping sweep to every possible address, and so reconnaissance will be tougher for the attacker using that method (because there are potentially millions of addresses on each subnet [264 possibilities, or about 18 quintillion!]).	Should Read: If an attacker issues a ping sweep of your network, he will not likely find all the devices via a traditional ping sweep to every possible address, so reconnaissance will be tougher for the attacker using that method (because there are potentially millions of addresses on each subnet [264 possibilities, or about 18 quintillion!]).

365	Chapter 14, Table 14-7, Second Feature, Second Explanation, Last Sentence Reads: With the additional features, more types of traffic can be classified and then permitted or denied based on policy.	Should read: With the additional features, more types of traffic can be classified, then permitted or denied based on policy.
374	Chapter 14, Second Paragraph, First Sentence Reads: As you can see, ACLs have many uses, and therefore many Cisco IOS Software commands accept a reference to an ACL in their command syntax.	Should read: As you can see, ACLs have many uses, therefore many Cisco IOS Software commands accept a reference to an ACL in their command syntax.
384	Chapter 15, Example 15-1, 15th Config Line Down Reads: R3(config-sec-zone)# **zone-pair security in-to-out source inside destination outside**	Should read: R3(config)# **zone-pair security in-to-out source inside destination outside**
479	Chapter 18, E-Mail-Based Threats, First Bullet Point, Second Sentence Reads: E-mail spam continuous to be a major threat because it can be used to spread malware.	Should read: E-mail spam continues to be a major threat because it can be used to spread malware.

479	Chapter 18, Cisco Cloud E-mail Security, First Sentence Reads: Cisco cloud e-mail security provides a cloud-based solution that allows companies to out-source the management of their e-mail security management.	Should read: Cisco cloud e-mail security provides a cloud-based solution that allows companies to out-source the management of their e-mail security.
491	Chapter 18, Cisco Content Security Management Appliance, Last Sentence Reads: Figure 18-8 shows a Cisco SMA that is controlling Cisco ESA and Cisco WSAs in different geographic locations (New York, Raleigh, Chicago, and Boston).	Should read: Figure 18-8 shows a Cisco SMA that is controlling Cisco ESAs and Cisco WSAs in different geographic locations (New York, Raleigh, Chicago, and Boston).
514	**CORRECTION TO ERRATA** **Appendix A, Chapter 17, Question 8, Answer wrong in below errata**	**Should read:** **8. A and B**

Corrections for January 18, 2016

Pg	**Error - First Printing**	**Correction**
xxvi	Introduction, Third Paragraph, Remove Second Sentence	Sentence to remove: The prerequisite for CCNA Security is the CCNA Route/Switch certification (or any CCIE certification).

11	Chapter 1, What Do We Do with the Risk?, Third Paragraph, Last sentence Reads: As mentioned in the previous paragraph, the risk assumed by the service provider is not completely eliminated, which results in residual risk that your organization must understood and accept.	Should read: As mentioned in the previous paragraph, the risk assumed by the service provider is not completely eliminated, which results in residual risk that your organization must understand and accept.
35	Chapter 3, First Paragraph, Remove First Sentence	Sentence to remove: As you learned in the preceding chapter, using *authentication*, *authorization*, and *accounting (AAA)* to verify the identity of a user, and what that user is authorized to do, is a great way to secure the management plane on a router or switch.
107	Chapter 5, Putting the Pieces of PKI to Work, Remove Second Sentence	Sentence to remove: What I want to do now is walk you through an example of applying these concepts to some devices you are already familiar with if you have read the previous portions of this book.
165	Chapter 7, First Paragraph, Third Sentence Reads: Because R1 is connected to the 172.16.0.0 network, we can craft a ping request sourced from that network (interface g2/0) and destined for the 192.168.0.2 address or R2, as shown in Example 7.5.	Should read: Because R1 is connected to the 172.16.0.0 network, we can craft a ping request sourced from that network (interface g1/0) and destined for the 192.168.0.2 address or R2, as shown in Example 7.5.

217	Chapter 8, Second Paragraph, First Sentence Reads: As you can see from the output, it gives information about the user who authenticated (which is a user I just created and name user1), that user's source IP address on the Internet, what time the user logged in, how long the user has been logged in, the encryption method that is in use, and the type of client.	Should read: As you can see from the output, it gives information about the user who authenticated (which is a user I just created and name omar), that user's source IP address on the Internet, what time the user logged in, how long the user has been logged in, the encryption method that is in use, and the type of client.

Corrections for December 14, 2015

Pg	Error - First Printing	Correction
342	Chapter 13, Question 5 Reads: **5.** In the following CoPP access control list example, which traffic is being prevented from reaching the control plane? Extended IP access list 123 10 deny tcp 192.168.1.0 0.0.0.25 any eq telent 20 deny udp 192.168.1.0 0.0.0.255 any eq domain 30 permit tcp any any eq telnet 40 permit udp any any eq domain 50 deny ip any any	Should read: **5.** In the following CoPP example, which traffic is being prevented from reaching the control plane? Extended IP access list 123 10 deny tcp 192.168.1.0 0.0.0.25 any eq telent 20 deny udp 192.168.1.0 0.0.0.255 any eq domain 30 permit tcp any any eq telnet 40 permit udp any any eq domain 50 deny ip any any Class-map match-all PEARSON match access-group 123 policy-map Pearson_Example

		class Pearson police 10000 5000 5000 conform-action DROP exceed-action drop
346	Chapter 13, Add Note Before Example 13-2	Note to be added: **NOTE** When constructing Access Control Lists (ACL) to be used for CoPP, traffic that is "permitted" translates to traffic that will be inspected by CoPP, and traffic that is "denied" translates to traffic that CoPP bypasses. Please refer to this white paper on CoPP: http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html. Specifically, see the following excerpt from the section, "Access List Construction": "There are several caveats and key points to keep in mind when constructing your access lists. • The **log** or **log-input** keywords must never be used in access-lists that are used within MQC policies for CoPP. The use of these keywords may cause unexpected result in the functionality of CoPP. • The use of the deny rule in access lists used in MQC is somewhat different to regular interface ACLs. Packets that match a deny rule are excluded from that class and cascade to the next class (if one exists) for classification. This is in contrast to packets matching a permit rule, which are then included in that class and no further comparisons are performed."
511	Appendix A, Chapter 1, Answer 4 Reads: **4.** B	Should read: **4.** B and D

Corrections for November 24, 2015

Pg	Error - First Printing	Correction
348	Chapter 13, Implementing Routing Update Authentication on OSPF, First Sentence Reads: MD5 authentication for OSPF requires configuration at both the interface level, that is, for each interface in which OSPF will be used, as well within the router OSPF process itself.	Should read: MD5 authentication for OSPF requires configuration at either the interface level, that is, for each interface in which OSPF will be used, or within the router OSPF process itself.
378	Chapter 15, Question 7 Reads: **7.** What doe the keyword *overload* imply in a NAT configuration?	Should read: **7.** What does the keyword *overload* imply in a NAT configuration?
410	Chapter 15, Table 15-6, Last Command Reads: **show ip nat translations***	Should read: **show ip nat translations**
488	Chapter 18, Last Paragraph Under Figure 18-5, First Sentence Reds: Figure 18-6 demonstrates how the WCCS registration works.	Should read: Figure 18-6 demonstrates how the WCCP registration works.

Corrections for November 16, 2015

Pg	Error - First Printing	Correction
322	Chapter 12, Question 9 Reads: **9.** Why is tunneling any protocol (including IPV6) through another protocol a security risk?	Should read: **9.** Why is tunneling any protocol (including IPV6) through another protocol a security risk? (Choose all that Apply.)
363	Chapter 14, Table 14-5, Column Disadvantages, Last Field, Second Sentence Reads: Could potentially be a single point of failure in the network, unlessv fault tolerance is also configured.	Should read: Could potentially be a single point of failure in the network, unless fault tolerance is also configured.
369	Chapter 14, Table 14-9, Column Description, Second Row, Second Sentence Reads: For example, a printer on the inside network may need to send packets out to the Internet, and as a result we will not use any global addresses (NAT or PAT) for that printer because the printer will never initiate traffic from the inside network going to the Internet.	Should read: For example, a printer on the inside network may not need to send packets out to the Internet, and as a result we will not use any global addresses (NAT or PAT) for that printer because the printer will never initiate traffic from the inside network going to the Internet.

Corrections for November 9, 2015

Pg	Error - First Printing	Correction
343	Chapter 13, Question 8, Answer C Reads: **c.** Router process (only for OSPF) must be configured; key chain in EIGRP	Should read: **c.** Router process or interface statement for OSPF must be configured; key chain in EIGRP
~~514~~	~~Appendix A, Chapter 17, Question 8, Answer~~ ~~Reads:~~ ~~8. A and B~~	~~Should read:~~ ~~8. A, B and C~~
514	Appendix A, Chapter 19, Question 3, Answer Reads: **3.** A	Should read: **3.** A and B

Corrections for October 21, 2015

Pg	Error - First Printing	Correction
41	Chapter 3, Third Paragraph, Fifth Sentence Reads: As done previously, comments about each of the commands and what their purpose is are included.	Should read: Comments about each of the commands and what their purpose is are included.

88	Chapter 5, Types of VPNs, Third Bullet Point, Last Sentence Reads: The primary VPNs that provide encryption, data integrity, authentication of who the peer is on the other end of the VPN, and so on useIPsec or SSL.	Should read: The primary VPNs that provide encryption, data integrity, authentication of who the peer is on the other end of the VPN, and so on use IPsec or SSL.
88	Chapter 5, Two Main Types of VPNs, First Bullet Point, Third Sentence Reads: Remote-access VPNs can use IPsec or *Secure Shell (SSL)* technologies for their VPN.	Should read: Remote-access VPNs can use IPsec or *Secure Sockets Layer (SSL)* technologies for their VPN.
94	Chapter 5, Hashes, Second Sentence Remove	Sentence to remove: Earlier in this chapter, we looked at a method for verifying the integrity of a downloaded IOS file from Cisco, and the method that was used was a hash.
457	Chapter 17, Cisco IDS/IPS Fundamentals, First Paragraph, Last Sentence Reads: This chapter focuses on the concepts of IPS/IDS in general, and then the next chapter examines the implementation of IPS/IDS as a software-based IOS solution.	Should read: This chapter focuses on the concepts of IPS/IDS in general.
512	Appendix A, Chapter 7, Answer to Question 11 Reads: **11.** A, B, C, and D	Should read: **11.** A and B

512	Appendix A, Chapter 9, Answer to Question 11 Reads: **11.** A	Should read: **11.** B

Corrections for September 1, 2015

Pg	Error - First Printing	Correction
337	Chapter 12, Example 12-4, Ninth Line Down Reads: CCNA-Router-1 (config-ipv6-acl)# **$1:DB8::100:1 2001:DB8:1:60::/64 eq 53**	Should read: CCNA-Router-1 (config-ipv6-acl)# **permit upd host 2001:DB8::100:1 2001:DB8:1:60::/64 eq 53**
346	Chapter 13, Control Plan Policing, Fourth Paragraph, First Sentence Reads: In Example 13-2, only BGP and *Secure Shell (SSH)* traffic from trusted hosts (that is, devices in the 192.168.1.0/24 subnet) is permitted to reach the Cisco IOS device CPU.	Should read: In Example 13-2, only Telnet and DNS traffic from trusted hosts (that is, devices in the 192.168.1.0/24 subnet) is permitted to reach the Cisco IOS device CPU.
381	Chapter 15, Figure 15-1, Router 3 (R3) Interface connecting to **Zone "DMZ"** Reads: G3/0 57.0.0.1	Should read: G2/0 57.0.0.1

This errata sheet is intended to provide updated technical information. Spelling and grammar misprints are updated during the reprint process, but are not listed on this errata sheet.