

Exam Checklist

CCNA Security Checklist Days 31–20		
Check Box	Date	Objective
		Schedule to take the CCNA Security IINS 210-260 Exam at http://www.vue.com .
		Take at least one CCNA Security practice exam.
		Describe confidentiality, integrity, availability, and SIEM.
		Identify common security terms and common security zones.
		Describe common network attacks, malware, and social engineering.
		Describe cryptographic key exchange, hash algorithms, digital signatures, certificates, and PKI.
		Describe network security architectures.
		Describe secure network management systems.
		Describe AAA concepts, such as RADIUS, TACACS+, ACS, and ISE.
		Describe the steps required to implement TACACS+.
		Describe 802.1X.
		Describe BYOD and MDM.
		Describe IPsec technologies and concepts.
		Describe the steps required to implement clientless SSL remote-access VPN.
		Describe the steps required to implement AnyConnect remote-access VPN.
		Read and review Days 31–20 in this book.

CCNA Security Checklist Days 19–10		
Check Box	Date	Objective
		Take an additional CCNA Security practice exam.
		Describe the steps required to implement a site-to-site VPN on an ASA and on an IOS router.
		Describe advanced VPN topics such as hairpinning, split tunneling, always-on, and NAT traversal.
		Describe how to implement secure device access with privilege levels and role-based CLI. Describe Cisco IOS resilient configuration.
		Describe how to secure network routing protocols.
		Describe and explain control plane policing.
		Describe STP attacks, ARP spoofing, MAC spoofing, CAM table attacks, CDP reconnaissance, VLAN hopping, and DHCP snooping.
		Describe how to implement DHCP snooping, DAI, port security, and STP protection mechanisms.
		Describe how to implement private VLANs and switch ACLs.

		Describe firewall technologies and operations.
		Describe the different types of ASA NAT implementations.
		Read and review Days 19–10 in this book.
CCNA Security Checklist Days 9–1		
Check Box	Date	Objective
		Take an additional CCNA Security practice exam.
		Describe how to implement an IOS Zone-Based Policy Firewall.
		Describe ASA firewall concepts, such as deployment modes, high availability, security contexts, and firewall services.
		Describe how to configure an ASA firewall, including access policies, access management, and MPP.
		Describe IDS and IPS concepts, such as deployment modes, placement, and alarms.
		Describe IDP and IPS technologies, such as rules, signatures, triggers, actions, and blacklisting.
		Describe email-based threat mitigation, such as SPAM filtering, malware filtering, and encryption.
		Describe web-based threat mitigation, such as local and cloud-based web proxies, URL filtering, web application filtering, and TLS/SSL decryption.
		Describe how to apply endpoint protection using antivirus, antimalware, firewalls, and encryption.
		Configure the network from Day 1, “CCNA Security Skills Review and Practice,” without using any references or the answer scripts.
		Read and review Days 9–1 in this book.
		Visit the testing center at least two days before the exam.
		Eat a healthy meal, go for a walk, and get a good night’s rest before the exam.