CCIE™ Security Written Exam Refresh v3.0(350-018)

andidates who have exams scheduled **August 12, 2010 or later** should prepare using the CCIE Security v3.0 Written Exam Topics (blueprints), Candidates **prior to August 11, 2010** should continue using the existing CCIE Security v2.0 Written Exam Topics. Please view the Written Exam Study/Learn tab for more information on how to study and prepare for the Written Exam. Please view the [Written Exam: Study/Learn](#) tab for more information on how to study and prepare for the Written Exam. The topic areas listed are general guidelines for the type of content that is likely to appear on the exam. Please note, however, that other relevant or related topic areas may also appear. The CCIE Security written exam for the v3.0 curriculum is a two-hour, multiple choice test with 100 questions covering the areas of skills and competency needed by a Security Engineer to implement, deploy, configure, maintain, and troubleshoot Cisco Network Security solutions and designs. Topics include Cisco network security devices, appliances, protocols, firewalls, VPNs, intrusion prevention devices, policy management, and best practices for implementing a secure network. All exam materials are provided and no outside reference materials are allowed. **1.00 General Networking ?** 1.10 Networking Basics (IPv4 and IPv6) 1.20 OSI Layers 1.30 TCP/IP Protocols 1.40 LAN Switching (e.g. VTP, VLANs, Spanning Tree, Trunking) 1.50 Routing Protocols (RIP, EIGRP, OSPF, and BGP) (IPv4 only) 1.60 Tunneling Protocols (GRE, NHRP) 1.70 IP Multicast **2.00 Security Protocols, Ciphers, Hashes, and Encryption** 2.01 Rivest, Shamir and Adleman (RSA) 2.02 Rivest Cipher 4 (RC4) 2.03 Message Digest 5 (MD5) 2.04 Secure Hash Algorithm (SHA) 2.05 Data Encryption Standard (DES) 2.06 Triple DES (3DES) 2.07 Advanced Encryption Standard (AES) 2.08 IP Security (IPsec) 2.09 Internet Security Association and Key Management Protocol (ISAKMP) 2.10 Internet Key Exchange (IKE) 2.11 Group Domain of Interpretation (GDOI) 2.12 Authentication Header (AH) 2.13 Encapsulating Security Payload (ESP) 2.14 Certificate Enrollment Protocol (CEP) 2.15 Transport Layer Security (TLS) 2.16 Secure Socket Layer (SSL) 2.17 Secure Shell (SSH) 2.18 Remote Authentication Dial In User Service (RADIUS) 2.19 Terminal Access Controller Access-Control System Plus (TACACS+) 2.20 Lightweight Directory Access Protocol (LDAP) 2.21 EAP Methods (e.g. EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, LEAP) **3.00 Application Protocols** 3.01 Hypertext Transfer Protocol (HTTP) 3.02 Hypertext Transfer Protocol Secure (HTTPS) 3.03 Simple Mail Transfer Protocol (SMTP) 3.04 Dynamic Host Configuration Protocol (DHCP) 3.05 Domain Name System (DNS) 3.06 File Transfer Protocol (FTP) 3.07 Trivial File Transfer Protocol (TFTP) 3.08 Network Time Protocol (NTP) 3.09 Simple Network Management Protocol (SNMP) 3.10 Syslog **4.00 Security Technologies** 4.01 Packet Filtering 4.02 Content Filtering 4.03 URL Filtering 4.04 Authentication Technologies 4.05 Authorization Technologies 4.06 Proxy Authentication 4.07 Public Key Infrastructure (PKI) 4.08 IPsec VPN 4.09 SSL VPN 4.10 Dynamic Multipoint VPN (DMVPN) 4.11 Group Encrypted Transport VPN (GET VPN) 4.12 Network Intrusion Prevention Systems 4.13 Host Intrusion Prevention Systems 4.14 Event Correlation 4.15 Network Admission Control (NAC) 4.16 802.1x 4.17 Endpoint Security 4.18 Network Address Translation (NAT) **5.00 Cisco Security Appliances and Applications** 5.01 Cisco Adaptive Security Appliance (ASA) Firewall 5.02 Cisco Intrusion Prevention System (IPS) 5.03 Cisco IOS Firewall (CBAC, Zone-Based, PAM) 5.04 Cisco IOS IPS 5.05 Cisco IOS AAA 5.06 Cisco IOS IPsec VPN 5.07 Cisco Easy VPN 5.08 Cisco SSL VPN 5.09 Cisco AnyConnect VPN Client 5.10 Cisco VPN Client 5.11 Cisco Secure Desktop (CSD) 5.12 Cisco Network Admission Control (NAC) Appliance 5.13 Cisco Security Agent (CSA) 5.14 Cisco Secure ACS for Windows 5.15 Cisco Secure ACS Solution Engine 5.16 Cisco Security Monitoring, Analysis and Response System (MARS) 5.17 Cisco Catalyst 6500 Series Security Services Modules (FWSM, IDSM-2, VPNSPA) **6.00 Cisco Security Management** 6.01 Cisco Adaptive Security Device Manager (ASDM) 6.02 Cisco Router & Security Device Manager (SDM) 6.03 Cisco Security Manager (CSM) 6.04 Cisco IPS Device Manager (IDM) 6.05 Cisco IPS Manager Express (IME) 6.06 Cisco Configuration Professional (CCP) **7.00 Cisco Security General** 7.01 Router Security Features (e.g. ACL, NBAR, MQC, CAR, FPM, uRPF, CoPP, CPPr, MPP) 7.02 Switch Security Features(e.g. IP & MAC Spoofing, MAC Address Controls, Port Security, DHCP Snooping, DNS Spoofing, ARP Spoofing, BPDU/Root Guard, PVLAN) 7.03 NetFlow 7.04 Wireless Security 7.05 IPv6 Security **8.00 Security Solutions** 8.01 Network Attack Mitigation 8.02 Virus and Worms Outbreaks 8.03 DoS/DDoS Attacks 8.04 Web Server & Web Application Security 8.05 DNS Security **9.00 Security General** 9.01 Security Policy 9.02 Information Security Standards (e.g. ISO/IEC 27001, ISO/IEC 27002) 9.03 Standards Bodies (e.g. ISO, IEC, ITU, ISOC, IETF, IAB, IANA, ICANN) 9.04 Industry/Regulatory Compliance (e.g. SOX, HIPAA, GLBA, PCI DSS, FISMA) 9.05 Common RFC/BCP (e.g. RFC1918, RFC3330, RFC2827/BCP38, RFC3704/BCP84, RFC2401) 9.06 Security Audit & Validation 9.07 Risk Assessment 9.08 Change Management Process 9.09 Incident Response Framework 9.10 Computer Security Forensics