CCIE Security Written Exam Blueprint v2.x

The Security written exam (350-018) has 100 multiple-choice questions and is two hours in duration. 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.

1. **General Networking**
    1. Networking Basics
    2. OSI Layers
    3. TCP/IP Protocols
    4. Switching (VTP, VLANs, Spanning Tree, Trunking, etc.)
    5. Routing Protocols (RIP, EIGRP, OSPF, and BGP)
    6. IP Multicast

2. **Security Protocols, Ciphers and Hash Algorithms**
    1. RADIUS
    2. TACACS+
    3. Ciphers RSA, DSS, RC4
    4. Message Digest 5 (MD5)
    5. Secure Hash Algorithm (SHA)
    6. EAP PEAP TKIP TLS
    7. Data Encryption Standard (DES)
    8. Triple DES (3DES)
    9. Advanced Encryption Standard (AES)
    10. IP Security (IPSec)
    11. Authentication Header (AH)
    12. Encapsulating Security Payload (ESP)
    13. Internet Key Exchange (IKE)
    14. Certificate Enrollment Protocol (CEP)
    15. Transport Layer Security (TLS)
    16. Secure Socket Layer (SSL)
    17. Point to Point Tunneling Protocol (PPTP)
    18. Layer 2 Tunneling Protocol (L2TP)
    19. Generic Route Encapsulation (GRE)
    20. Secure Shell (SSH)
    21. Pretty Good Privacy (PGP)

3. **Application Protocols**
    1. Hypertext Transfer Protocol (HTTP)
    2. Simple Mail Transfer Protocol (SMTP)
    3. File Transfer Protocol (FTP)
    4. Domain Name System (DNS)
    5. Trivial File Transfer Protocol (TFTP)
    6. Network Time Protocol (NTP)
    7. Lightweight Directory Access Protocol (LDAP)
    8. Syslog

4. **Security Technologies**
    1. Packet Filtering
    2. Content Filtering
    3. URL Filtering

4. Authentication Technologies
5. Authorization technologies
6. Proxy Authentication
7. Public Key Infrastructure (PKI)
8. IPSec VPN
9. SSL VPN
10. Network Intrusion Prevention Systems
11. Host Intrusion Prevention Systems
12. Event Correlation
13. Adaptive Threat Defense (ATD)
14. Network Admission Control (NAC)
15. 802.1x
16. Endpoint Security
17. Network Address Translation

5. Cisco Security Appliances and Applications

1. Cisco Secure PIX Firewall
2. Cisco Intrusion Prevention System (IPS)
3. Cisco VPN 3000 Series Concentrators
4. Cisco EzVPN Software and Hardware Clients
5. Cisco Adaptive Security Appliance (ASA) Firewall
6. Cisco Security Monitoring, Analysis and Response System (MARS)
7. Cisco IOS Firewall
8. Cisco IOS Intrusion Prevention System
9. Cisco IOS IPSec VPN
10. Cisco IOS Trust and Identity
11. Cisco Secure ACS for Windows
12. Cisco Secure ACS Solution Engine
13. Cisco Traffic Anomaly Detectors
14. Cisco Guard DDoS Mitigation Appliance
15. Cisco Catalyst 6500 Series Security Modules (FWSM, IDSM, VPNSM, WebVPN, SSL modules)
16. Cisco Traffic Anomaly Detector Module & Cisco Guard Service Module

6. Cisco Security Management

1. Cisco Adaptive Security Device Manager (ASDM)
2. Cisco Router & Security Device Manager (SDM)
3. Cisco Security Manager (CSM)

7. Cisco Security General

1. IOS Specifics
2. Routing and Switching Security Features: IP & MAC Spoofing, MAC Address Controls, Port Security, DHCP Snoop, DNS Spoof.
3. NetFlow
4. Layer 2 Security Features
5. Layer 3 Security Features
6. Wireless Security
7. IPv6 Security

8. Security Solutions

1. Network Attack Mitigation
2. Virus and Worms Outbreaks

3. Theft of Information
4. DoS/DDoS Attacks
5. Web Server & Web Application Security

9. Security General

1. Policies - Security Policy Best Practices
2. Information Security Standards (ISO 17799, ISO 27001, BS7799)
3. Standards Bodies
4. Common RFCs (e.g. RFC1918, RFC2827, RFC2401)
5. BCP 38
6. Attacks, Vulnerabilities and Common Exploits - recon, scan, priv escalation, penetration, cleanup, backdoor
7. Security Audit & Validation
8. Risk Assessment
9. Change Management Process
10. Incident Response Framework
11. Computer Security Forensics