

CCIE Security Written Exam

I. **General Networking**

- A. Networking Basics
- B. OSI Layers
- C. TCP/IP Protocols
- D. Switching (VTP, VLANs, Spanning Tree, Trunking, etc.)
- E. Routing Protocols (RIP, EIGRP, OSPF, and BGP)
- F. IP Multicast

II. **Security Protocols, Ciphers and Hash Algorithms**

- A. RADIUS
- B. TACACS+
- C. Ciphers RSA, DSS, RC4
- D. Message Digest 5 (MD5)
- E. Secure Hash Algorithm (SHA)
- F. EAP PEAP TKIP TLS
- G. Data Encryption Standard (DES)
- H. Triple DES (3DES)
- I. Advanced Encryption Standard (AES)
- J. IP Security (IPSec)
- K. Authentication Header (AH)
- L. Encapsulating Security Payload (ESP)
- M. Internet Key Exchange (IKE)
- N. Certificate Enrollment Protocol (CEP)
- O. Transport Layer Security (TLS)
- P. Secure Socket Layer (SSL)
- Q. Point to Point Tunneling Protocol (PPTP)
- R. Layer 2 Tunneling Protocol (L2TP)
- S. Generic Route Encapsulation (GRE)
- T. Secure Shell (SSH)
- U. Pretty Good Privacy (PGP)

III. **Application Protocols**

- A. Hypertext Transfer Protocol (HTTP)

- B. Simple Mail Transfer Protocol (SMTP)
- C. File Transfer Protocol (FTP)
- D. Domain Name System (DNS)
- E. Trivial File Transfer Protocol (TFTP)
- F. Network Time Protocol (NTP)
- G. Lightweight Directory Access Protocol (LDAP)
- H. Syslog

IV. Security Technologies

- A. Packet Filtering
- B. Content Filtering
- C. URL Filtering
- D. Authentication Technologies
- E. Authorization technologies
- F. Proxy Authentication
- G. Public Key Infrastructure (PKI)
- H. IPSec VPN
- I. SSL VPN
- J. Network Intrusion Prevention Systems
- K. Host Intrusion Prevention Systems
- L. Event Correlation
- M. Adaptive Threat Defense (ATD)
- N. Network Admission Control (NAC)
- O. 802.1x
- P. Endpoint Security
- Q. Network Address Translation

V. Cisco Security Appliances and Applications

- A. Cisco Secure PIX Firewall
- B. Cisco Intrusion Prevention System (IPS)
- C. Cisco VPN 3000 Series Concentrators
- D. Cisco EzVPN Software and Hardware Clients
- E. Cisco Adaptive Security Appliance (ASA) Firewall
- F. Cisco Security Monitoring, Analysis and Response System (MARS)
- G. Cisco IOS Firewall
- H. Cisco IOS Intrusion Prevention System

- I. Cisco IOS IPSec VPN
- J. Cisco IOS Trust and Identity
- K. Cisco Secure ACS for Windows
- L. Cisco Secure ACS Solution Engine
- M. Cisco Traffic Anomaly Detectors
- N. Cisco Guard DDoS Mitigation Appliance
- O. Cisco Catalyst 6500 Series Security Modules (FWSM, IDSM, VPNSM, WebVPN, SSL modules)
- P. Cisco Traffic Anomaly Detector Module & Cisco Guard Service Module

VI. Cisco Security Management

- A. Cisco Adaptive Security Device Manager (ASDM)
- B. Cisco Router & Security Device Manager (SDM)
- C. Cisco Security Manager (CSM)

VII. Cisco Security General

- A. IOS Specifics
- B. Routing and Switching Security Features: IP & MAC Spoofing, MAC Address Controls, Port Security, DHCP Snoop, DNS Spoof.
- C. NetFlow
- D. Layer 2 Security Features
- E. Layer 3 Security Features
- F. Wireless Security
- G. IPv6 Security

VIII. Security Solutions

- A. Network Attack Mitigation
- B. Virus and Worms Outbreaks
- C. Theft of Information
- D. DoS/DDoS Attacks
- E. Web Server & Web Application Security

IX. Security General

- A. Policies - Security Policy Best Practices
- B. Information Security Standards (ISO 17799, ISO 27001, BS7799)
- C. Standards Bodies

- D. Common RFCs (e.g. RFC1918, RFC2827, RFC2401)
- E. BCP 38
- F. Attacks, Vulnerabilities and Common Exploits - recon, scan, priv escalation, penetration, cleanup, backdoor
- G. Security Audit & Validation
- H. Risk Assessment
- I. Change Management Process
- J. Incident Response Framework
- K. Computer Security Forensics