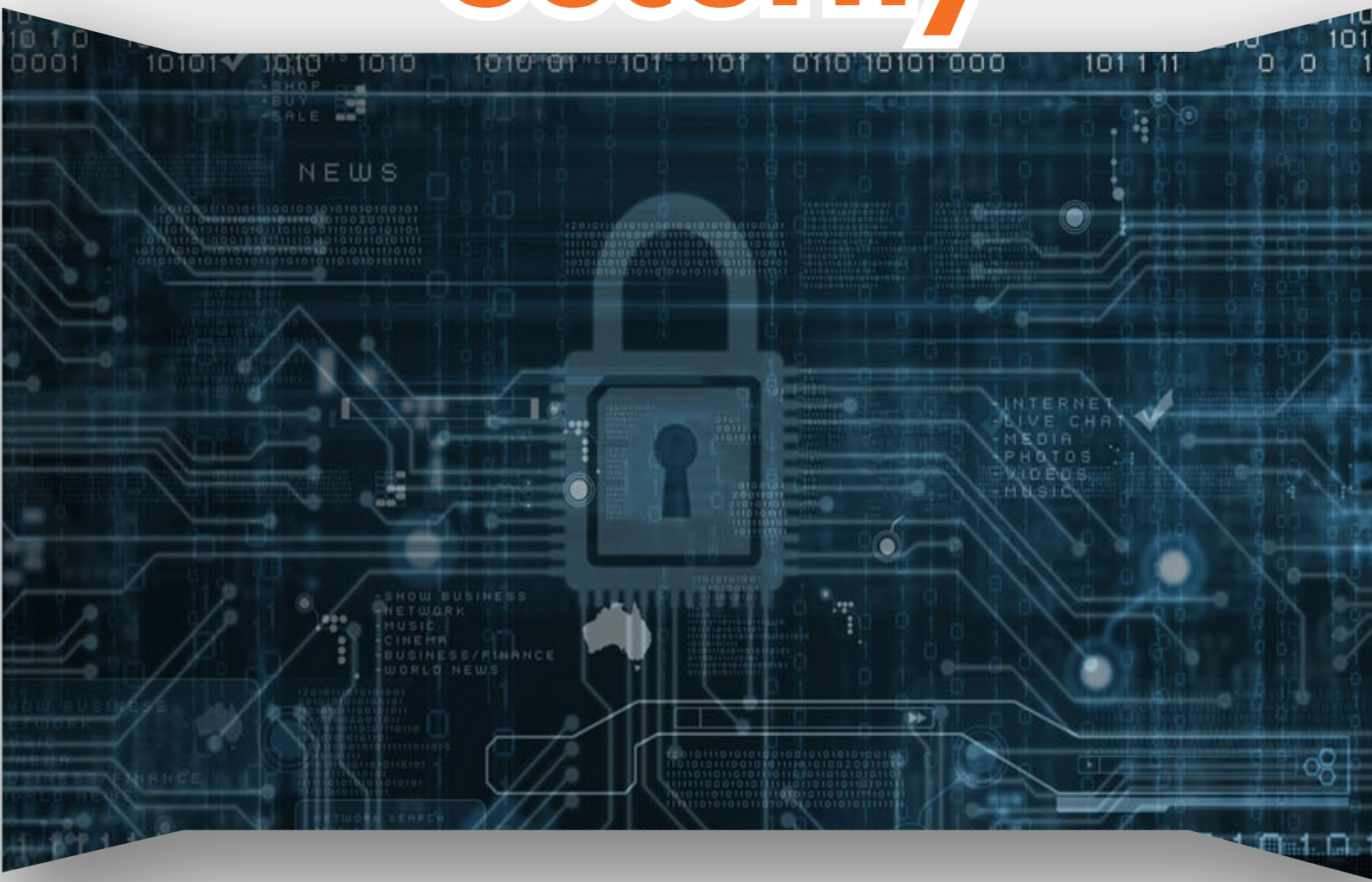
CCNA Security

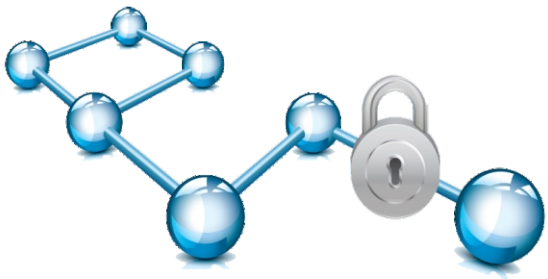


SevenMentor PVT.LTD

Implementing Cisco Network Security Exam (210-260)

Exam Description: The Implementing Cisco Network Security (IINS) exam (210-260) is a 90-minute assessment with 60 to 70 questions. This exam tests the candidate's knowledge of secure network infrastructure, understanding core security concepts, managing secure access, VPN encryption, firewalls, intrusion prevention, web and email content security, and endpoint security. This exam validates skills for installation, troubleshooting, and monitoring of a secure network to maintain integrity, confidentiality, and availability of data and devices. This exam also shows competency in the technologies that Cisco uses in its security infrastructure. Candidates can prepare for this exam by taking the Implementing Cisco Network Security (IINS) course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.



CISCO SECURITY

SevenMentor PVT.LTD

12% 1.0 Security Concepts
14% 2.0 Secure Access
17% 3.0 VPN
18% 4.0 Secure Routing and Switching
18% 5.0 Cisco Firewall Technologies
09% 6.0 IPS
12% 7.0 Content and Endpoint Security

1.0 Security Concepts

1.1 Common security principles
- 1.1.1 Describe confidentiality, integrity, availability (CIA)
- 1.1.2 Describe SIEM technology
- 1.1.3 Identify common security terms
- 1.1.4 Identify common network security zones

1.2 Common security threats
- 1.2.1 Identify common network attacks
- 1.2.2 Describe social engineering
- 1.2.3 Identify malware
- 1.2.4 Classify the vectors of data loss/exfiltration

1.3 Cryptography concepts
- 1.3.1 Describe key exchange
- 1.3.2 Describe hash algorithm
- 1.3.3 Compare and contrast symmetric and asymmetric encryption
- 1.3.4 Describe digital signatures, certificates, and PKI

1.4 Describe network topologies
- 1.4.1 Campus area network (CAN)
- 1.4.2 Cloud, wide area network (WAN)
- 1.4.3 Data center
- 1.4.4 Small office/home office (SOHO)
- 1.4.5 Network security for a virtual environment

2.0 Secure Access

2.1 Secure management
- 2.1.1 Compare in-band and out-of band
- 2.1.2 Configure secure network management
- 2.1.3 Configure and verify secure access through SNMP v3 using an ACL
- 2.1.4 Configure and verify security for NTP
- 2.1.5 Use SCP for file transfer

2.2 AAA concepts
- 2.2.1 Describe RADIUS and TACACS+ technologies
- 2.2.2 Configure administrative access on a Cisco router using TACACS+
- 2.2.3 Verify connectivity on a Cisco router to a TACACS+ server
- 2.2.4 Explain the integration of Active Directory with AAA
- 2.2.5 Describe authentication and authorization using ACS and ISE

2.3 802.1X authentication
- 2.3.1 Identify the functions 802.1X components

2.4 BYOD
- 2.4.1 Describe the BYOD architecture framework
- 2.4.2 Describe the function of mobile device management (MDM)

3.0 VPN

3.1 VPN concepts
- 3.1.1 Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
- 3.1.2 Describe hair pinning, split tunneling, always-on, NAT traversal

3.2 Remote access VPN
- 3.2.1 Implement basic clientless SSL VPN using ASDM
- 3.2.2 Verify clientless connection
- 3.2.3 Implement basic AnyConnect SSL VPN using ASDM
- 3.2.4 Verify AnyConnect connection
- 3.2.5 Identify endpoint posture assessment

3.3 Site-to-site VPN
- 3.3.1 Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
- 3.3.2 Verify an IPsec site-to-site VPN

4.0 Secure Routing and Switching

4.1 Security on Cisco routers
- 4.1.1 Configure multiple privilege levels
- 4.1.2 Configure Cisco IOS role-based CLI access
- 4.1.3 Implement Cisco IOS resilient configuration

4.2 Securing routing protocols
- 4.2.1 Implement routing update authentication on OSPF

4.3 Securing the control plane
- 4.3.1 Explain the function of control plane policing

4.4 Common Layer 2 attacks
- 4.4.1 Describe STP attacks
- 4.4.2 Describe ARP spoofing
- 4.4.3 Describe MAC spoofing
- 4.4.4 Describe CAM table (MAC address table) overflows
- 4.4.5 Describe CDP/LLDP reconnaissance
- 4.4.6 Describe VLAN hopping
- 4.4.7 Describe DHCP spoofing

4.5 Mitigation procedures
- 4.5.1 Implement DHCP snooping
- 4.5.2 Implement Dynamic ARP Inspection
- 4.5.3 Implement port security
- 4.5.4 Describe BPDU guard, root guard, loop guard
- 4.5.5 Verify mitigation procedures

4.6 VLAN security
- 4.6.1 Describe the security implications of a PVLAN
- 4.6.2 Describe the security implications of a native VLAN

5.0 Cisco Firewall Technologies

5.1 Describe operational strengths and weaknesses of the different firewall technologies
- 5.1.1 Proxy firewalls
- 5.1.2 Application firewall
- 5.1.3 Personal firewall

5.2 Compare stateful vs. stateless firewalls
- 5.2.1 Operations
- 5.2.2 Function of the state table

5.3 Implement NAT on Cisco ASA 9.x
- 5.3.1 Static
- 5.3.2 Dynamic
- 5.3.3 PAT
- 5.3.4 Policy NAT
- 5.3.5 Verify NAT operations

5.4 Implement zone-based firewall
5.4.1 Zone to zone
5.4.2 Self zone

5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
5.5.1 Configure ASA access management
5.5.2 Configure security access policies
5.5.3 Configure Cisco ASA interface security levels
5.5.4 Configure default Cisco Modular Policy Framework (MPF)
5.5.5 Describe modes of deployment (routed firewall, transparent firewall)
5.5.6 Describe methods of implementing high availability
5.5.7 Describe security contexts
5.5.8 Describe firewall services

6.0 IPS

6.1 Describe IPS deployment considerations
6.1.1 Network-based IPS vs. host-based IPS
6.1.2 Modes of deployment (inline, promiscuous - SPAN, tap)
6.1.3 Placement (positioning of the IPS within the network)
6.1.4 False positives, false negatives, true positives, true negatives

6.2 Describe IPS technologies
6.2.1 Rules/signatures
6.2.2 Detection/signature engines
6.2.3 Trigger actions/responses (drop, reset, block, alert, monitor/log, shun) 6.2.d
6.2.4 Blacklist (static and dynamic)

7.0 Content and Endpoint Security

7.1 Describe mitigation technology for email-based threats
- A. SPAM filtering, anti-malware filtering, DLP, blacklisting email encryption

7.2 Describe mitigation technology for web-based threats
- 7.2.1 Local and cloud-based web proxies
- 7.2.2 Blacklisting, URL filtering, malware scanning, URL categorization web application filtering, TLS/SSL decryption

7.3 Describe mitigation technology for endpoint threats
- 7.3.1 Anti-virus/anti-malware
- 7.3.2 Personal firewall/HIPS
- 7.3.3 Hardware/software encryption of local data