



Cisco Network Security Specialist v1.0 (500-750)

Exam Description: Cisco Network Security Specialist v1.0 (CNSS 500-750) is a 90-minute exam that tests a candidate's knowledge and skills related to secure network infrastructure, understanding core security concepts, managing secure access, VPN encryption, firewalls, intrusion prevention, web and email content security, and endpoint security. The course, Implementing Cisco Network Security (IINS), helps candidates prepare for this exam.

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. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

- 12%** **1.0** **Security Concepts**
 - 1.1 Common security principles
 - 1.1.a Describe Confidentiality, Integrity, Availability (CIA)
 - 1.1.b Describe SIEM technology
 - 1.1.c Identify common security terms
 - 1.1.d Identify common network security zones
 - 1.2 Common security threats
 - 1.2.a Identify common network attacks
 - 1.2.b Describe social engineering
 - 1.2.c Identify malware
 - 1.2.d Classify the vectors of data loss/exfiltration
 - 1.3 Cryptography concepts
 - 1.3.a Describe key exchange
 - 1.3.b Describe hash algorithm
 - 1.3.c Compare & contrast symmetric and asymmetric encryption
 - 1.3.d Describe digital signatures, certificates and PKI
 - 1.4 Describe network topologies
 - 1.4.a Campus Area Network (CAN)
 - 1.4.b Cloud, Wide Area Network (WAN)
 - 1.4.c Data Center
 - 1.4.d Small office/home office (SOHO)
 - 1.4.e Network security for a virtual environment
- 14%** **2.0** **Secure Access**
 - 2.1 Secure management
 - 2.1.a Compare In-band and out of band
 - 2.1.b Configure secure network management

- 2.1.c Configure and verify secure access through SNMP v3 using an ACL
- 2.1.d Configure and verify security for NTP
- 2.1.e Use SCP for file transfer
- 2.2 AAA concepts
 - 2.2.a Describe RADIUS & TACACS+ technologies
 - 2.2.b Configure administrative access on a Cisco router using TACACS+
 - 2.2.c Verify connectivity on a Cisco router to a TACACS+ server
 - 2.2.d Explain the integration of Active Directory with AAA
 - 2.2.e Describe authentication & authorization using ACS and ISE
- 2.3 802.1X authentication
 - 2.3.a Identify the functions 802.1X components
- 2.4 BYOD
 - 2.4.a Describe the BYOD architecture framework
 - 2.4.b Describe the function of Mobile Device Management (MDM)
- 17%** **3.0 VPN**
 - 3.1 VPN concepts
 - 3.1.a Describe IPSec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
 - 3.1.b Describe hairpinning, split tunneling, always-on, NAT Traversal
 - 3.2 Remote Access VPN
 - 3.2.a Implement basic clientless SSL VPN using ASDM
 - 3.2.b Verify clientless connection
 - 3.2.c Implement basic AnyConnect SSL VPN using ASDM
 - 3.2.d Verify AnyConnect connection
 - 3.2.e Identify Endpoint Posture Assessment
 - 3.3 Site-to-Site VPN
 - 3.3.a Implement an IPSec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
 - 3.3.b Verify an IPSec site-to-site VPN
- 18%** **4.0 Secure Routing & Switching**
 - 4.1 Security on Cisco Routers
 - 4.1.a Configure multiple privilege levels
 - 4.1.b Configure IOS role-based CLI access
 - 4.1.c Implement IOS resilient configuration
 - 4.2 Securing routing protocols
 - 4.2.a Implement routing update authentication on OSPF
 - 4.3 Securing the control plane
 - 4.3.a Explain the function of control plane policing

- 4.4 Common Layer 2 attacks
 - 4.4.a Describe STP attacks
 - 4.4.b Describe ARP spoofing
 - 4.4.c Describe MAC spoofing
 - 4.4.d Describe CAM Table (MAC Address Table) overflows
 - 4.4.e Describe CDP/LLDP reconnaissance
 - 4.4.f Describe VLAN hopping
 - 4.4.g Describe DHCP spoofing
- 4.5 Mitigation procedures
 - 4.5.a Implement DHCP snooping
 - 4.5.b Implement dynamic ARP inspection
 - 4.5.c Implement port security
 - 4.5.d Describe BPDU Guard, Root Guard, Loop Guard
 - 4.5.e Verify mitigation procedures
- 4.6 VLAN security
 - 4.6.a Describe the security implications of a PVLAN
 - 4.6.b Describe the security implications of a native VLAN
- 18% 5.0 Cisco Firewall Technologies**
 - 5.1 Describe operational strengths and weaknesses of the different firewall technologies
 - 5.1.a Proxy firewalls
 - 5.1.b Application firewall
 - 5.1.c Personal firewall
 - 5.2 Compare stateful vs. stateless firewalls
 - 5.2.a Operations
 - 5.2.b Function of the state table
 - 5.3 Implement NAT on Cisco ASA 9.x
 - 5.3.a Static
 - 5.3.b Dynamic
 - 5.3.c PAT
 - 5.3.d Policy NAT
 - 5.3 e Verify NAT operations
 - 5.4 Implement zone-based firewall
 - 5.4.a Zone to zone
 - 5.4.b Self zone
 - 5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
 - 5.5.a Configure ASA Access Management
 - 5.5.b Configure security access policies
 - 5.5.c Configure Cisco ASA interface security levels
 - 5.5.d Configure default Modular Policy Framework (MPF)
 - 5.5.e Describe modes of deployment (routed firewall, transparent firewall)
 - 5.5.f Describe methods of implementing High Availability

- 5.5.g Describe security contexts
- 5.5.h Describe firewall services

9% 6.0 IPS

- 6.1 Describe IPS deployment considerations
 - 6.1.a Network based IPS vs. host based IPS
 - 6.1.b Modes of deployment (inline, promiscuous - SPAN, tap)
 - 6.1.c Placement (positioning of the IPS within the network)
 - 6.1.d False positives, false negatives, true positives, true negatives

- 6.2 Describe IPS technologies
 - 6.2.a Rules/Signatures
 - 6.2.b Detection/Signature engines
 - 6.2.c Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)
 - 6.2.d Block list (static & dynamic)

12% 7.0 Content and Endpoint Security

- 7.1 Describe mitigation technology for email-based threats
 - 7.1.a SPAM filtering, anti-malware filtering, DLP, block listing, email encryption

- 7.2 Describe mitigation technology for Web-based threats
 - 7.2.a Local & cloud-based Web proxies
 - 7.2.b Block listing, URL-filtering, malware scanning, URL categorization, Web application filtering, TLS/SSL decryption

- 7.3 Describe mitigation technology for endpoint threats
 - 7.3.a Anti-Virus/Anti-Malware
 - 7.3.b Personal Firewall/HIPS
 - 7.3.c Hardware/Software encryption of local data