Course Description

CTS2664 | CISCO Certified Network Associate (CCNA) Security |4.00 credits
This course is designed for students specializing in Cisco Network Security. Students will learn how to master core security concepts, secure network infrastructure, manage secure access, recognize threats and vulnerabilities, and mitigate security threats. The course prepares students for the Cisco IINS Exam 210-260 certification. Prerequisite: CTS1651.

Course Competencies:
Competency 1: The student will demonstrate an understanding of basic security concepts by:

1. Defining standard security terms
2. Describing confidentiality, integrity, and availability
3. Identifying the different types of social engineering techniques
4. Explaining the uses of Security Information and Event Management (SIEM) technology
5. Identifying common types of network attacks, security threats, and network security zones
6. Comparing and contrasting symmetric and asymmetric encryption
7. Describing digital signatures, certificates, and PKI, key exchange, hashing
8. Identifying network topologies: campus area network (CAN), vast area network (WAN), Small Office Home Office (SOHO), Data Center, Virtual

Competency 2: The student will demonstrate an understanding of secure access management by:

1. Comparing in-band and out-of-band access
2. Configuring secure network management
3. Using Secure Copy Protocol (SCP) for file transfer
4. Configuring and verifying secure access through Simple Network Management Protocol (SNMP) v3
5. using an Access Control List (ACL) and Network Time Protocol (NTP)
6. Describing Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) technologies
7. Configuring and verifying access on a Cisco router using TACACS+
8. Explaining the integration of Active Directory with Authentication, Authorization, and Accounting (AAA)
9. Describing authentication and authorization using an Access Control Server (ACS) and Identity Services Engine (ISE)
10. Identifying the functions of 802.1X components
11. Analyzing the Bring Your Device (BYOD) architecture framework
12. Describing the function of mobile device management (MDM)

Competency 3: The student will demonstrate an understanding of the Virtual Private Network (VPN) concepts of remote assess VPN and site-to-site VPN by:

1. Describing Internet Protocol Security (IPsec) protocols and delivery modes, e.g., Internet Key Exchange (IKE) Encapsulating Security Payload (ESP), Authentication Header (AH), tunnel and transport mode
2. Defining and explaining the functions of hair pinning, split tunneling, always-on, Network Address Translation (NAT), traversal
3. Configuring basic clientless Secure Sockets Layer (SSL) ACS VPN using Adaptive Security Device Manager (ASDM)
4. Verifying clientless connection and AnyConnect access
5. Identifying endpoint posture assessment
6. Implementing an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and Adaptive Security Appliance (ASA) firewalls
7. Verifying an IPsec site-to-site VPN

Competency 4: The student will demonstrate an understanding of securing Cisco routers, routing protocols, control plane, layer two attacks, mitigation procedures, and virtual local area network (VLAN) security by:

1. Configuring multiple privilege levels and Internetwork Operating System (IOS) role-based Command Line Interface (CLI) access
2. Implementing Cisco IOS resilient configuration

3. Implementing routing update authentication on Open Shortest Path First (OSPF)
4. Explaining the functions of control plane policing
5. Differentiating between Spanning Tree Protocol (STP) attacks, Address Resolution Protocol (ARP), Media Access Control (MAC), Dynamic Host Configuration Protocol (DHCP), spoofing
6. Defining Cisco Discovery Protocol / Link Layer Discovery Protocol (CDP/LLDP) reconnaissance, VLAN hopping, Bridge Protocol Data Units (BPDU) guard, root guard, loop guard
7. Implementing DHCP snooping, ARP Inspection, Port security
8. Comparing and contrasting the security implications of a Private VLAN (PVLAN) and a native VLAN

Competency 5: The student will demonstrate an understanding of Cisco firewall technologies by:

1. Describing the operational strengths and weaknesses of Proxy, Application, and Personal firewall technologies
2. Comparing stateful vs. stateless firewall operations and function of the state table
3. Implementing and verifying NAT on Cisco Adaptive Security Appliance (ASA)
4. using both Static and Dynamic NAT, with Port Address Translation (PAT)
5. Implementing zone-based firewall (Zone to zone, Self-zone)
6. Delineating Firewall features on the Cisco ASA
7. Configuring ASA access management, ASA interface security levels, security access policies, default Cisco Modular Policy Framework (MPF)
8. Selecting appropriate modes of deployment (e.g., routed firewall, transparent firewall)
9. Describing methods of implementing high-availability
10. Discussing security contexts and firewall services

Competency 6: The student will demonstrate an understanding of the Cisco Intrusion Prevention System (IPS) by:

1. Assessing IPS deployment considerations
2. Differentiating between Network-based IPS vs. host-based IPS
3. Defining false positives, false negatives, true positives, and true negatives
4. Describing modes of deployment, including inline, promiscuous - Switched Port Analyzer (SPAN), and tap
5. Describing IPS technologies of rules, detection, trigger actions, and static and dynamic blacklist

Competency 7: The student will demonstrate an understanding of content and endpoint security by:

1. Describing mitigation technology for email-based threats
2. Differentiating between spam filtering, anti-malware filtering, Data Loss Prevention (DLP), blacklisting, email encryption
3. Describing mitigation technology for web-based threats
4. Identifying Uniform Resource Locator (URL) filtering, malware scanning, URL categorization, web application filtering, and Transport Layer Security/Secure Socket Layer (TLS/SSL) decryption
5. Describing mitigation technology for endpoint threats
6. Configuring anti-virus/anti-malware, personal firewall/host-based intrusion prevention systems (HIPS)
7. Explaining the steps involved in how to enable hardware/software encryption of local data.

<u>Learning Outcomes:</u>

- Solve problems using critical and creative thinking and scientific reasoning
- Use computer and emerging technologies effectively

Updated: Fall 2025