CloudSystems Limited
Ka-57/1, Kazi Tower 3rd Floor,
Kuril Bus Stand, Dhaka-1229.
☎ +880 1712900654

CCNA Security (210-260)

Overview:

This course is comprised of the CISCO CCNA Security Curriculum. The CCNA Security curriculum prepares students for the Implementing CISCO IOS Network Security (IINS) certification exam (210-260), leading to the CCNA Security certification.

CCNA Security course is the ultimate training program for engineers pursuing the Cisco Certified Network Associate Security (CCNA Security) certification. Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats.

Course Objectives:

On completion of this course, students should have the skills to:

- Describe the security threats facing modern network infrastructures
- Secure network device access
- Implement AAA on network devices
- Mitigate threats to networks using ACLs
- Cryptography
- Content and endpoint security
- Mitigate common Layer 2 attacks
- Implement the CISCO IOS firewall feature set
- Implement the CISCO IOS IPS feature set
- Implement VPN Technology.
- Administer effective security policies

Who should attend?

The target audience for this course is:

- IT networking professionals.
- People with a background in deploying and supporting networking infrastructure (routers and switches).
- CCNA Security provides a next step for CCNA Routing & Switching who want to expand their network protection skill to prepare for a career in network security.

Prerequisites:

It is recommended that students have a technical background in networking, particularly routers & switches. This may be achieved by at least a year working with routers at the command line and/or completing a recent CISCO CCNA course.

Course Duration:

40 Hours

CloudSystems Limited
Ka-57/1, Kazi Tower 3rd Floor,
Kuril Bus Stand, Dhaka-1229.
☎ +880 1712900654

Course Content:

Lesson 01: Security Concepts

- Common security principles
- Describe confidentiality, integrity, availability (CIA)
- Describe SIEM technology
- Identify common security terms
- Identify common network security zones

Lesson 02: Common security threats

- Identify common network attacks
- Describe social engineering
- Identify malware
- Classify the vectors of data loss/exhilaration

Lesson 03: Cryptography concepts

- Describe key exchange
- Describe hash algorithm
- Compare and contrast symmetric and asymmetric encryption
- Describe digital signatures, certificates, and PKI

Lesson 04: Describe network topologies

- Campus area network (CAN)
- Cloud, Wide area network(WAN)
- Data center
- Small Office/home office(SOHO)
- Network security for a environment

Lesson 05: Secure management

- Compare in-band and out-of band
- Configure secure network management
- Configure and verify secure access through SNMP v3 using an ACL
- Configure and verify security for NTP
- Use SCP for file transfer

Lesson 06: AAA concepts

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

Lesson 07: 802.1X authentication

- Identify the functions 802.1X components
- Describe the function of mobile device management (MDM)
- Describe the BYOD architecture framework

Lesson 08: VPN

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

Lesson 09: Remote access VPN

- Implement basic clientless SSL VPN using ASDM
- Verify clientless connection
- Implement basic Any Connect SSL VPN using ASDM
- Verify Any Connect connection
- Identify endpoint posture assessment

Lesson 10: Site-to-site VPN

- Implement an IP sec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
- Verify an IP sec site-to-site VPN

Lesson 11: Secure Routing and Switching

- Configure multiple privilege levels
- Configure Cisco IOS role-based CLI access
- Implement Cisco IOS resilient configuration

Lesson 12: Securing routing protocols

- Implement routing update authentication on OSPF

Lesson 13: Securing the control plane

- Explain the function of control plane policing

Lesson 14: Common Layer 2 attacks

- Describe STP attacks
- Describe ARP spoofing
- Describe MAC spoofing
- Describe CAM table (MAC address table) overflows
- Describe CDP/LLDP reconnaissance
- Describe VLAN hopping
- Describe DHCP spoofing

CloudSystems Limited
Ka-57/1, Kazi Tower 3rd Floor,
Kuril Bus Stand, Dhaka-1229.
☎ +880 1712900654

Lesson 15: Mitigation procedures

- Implement DHCP snooping
- Implement Dynamic ARP Inspection
- Implement port security
- Describe BPDU guard, root guard, loop guard
- Verify mitigation procedures

Lesson 16: VLAN security

- Describe the security implications of a PVLAN
- Describe the security implications of a native VLAN

Lesson 17: Cisco Firewall Technologies

- Describe operational strengths and weaknesses of the different firewall technologies
- Proxy firewalls
- Application firewall
- Personal firewall

Lesson 18: Compare stateful vs. stateless firewalls

- Operations
- Function of the state table

Lesson 19: Implement NAT on Cisco ASA 9.x

- Static
- Dynamic
- PAT
- Policy NAT
- Verify NAT operations-based firewall
- Zone to zone
- Self-zone

Lesson 20: Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x

- Configure ASA access management
- Configure security access policy
- Configure Cisco ASA interface security levels
- Configure default Cisco Modular Policy Framework (MPF)
- Describe modes of deployment (routed firewall, transparent firewall)
- Describe methods of implementing high availability
- Describe security contexts
- Describe firewall services

Lesson 21: Describe IPS deployment Network-based IPS vs. host-based IPS

- Modes of deployment (inline, promiscuous - SPAN, tap)
- Placement (positioning of the IPS within the network)
- False positives, false negatives, true positives, true negatives

Lesson 22: Describe IPS technologies

- Rules/signatures
- Detection/signature engines
- Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)
- Blacklist (static and dynamic)

Lesson 23: Describe mitigation technology for email-

- SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption

Lesson 24: Describe mitigation technology for web-based threats

- Local and cloud-based web proxies
- Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption

Lesson 25: Describe mitigation technology for email-based threats

- Anti-virus/anti-malware
- Personal firewall/HIPS
- Hardware/software encryption of local data