Training Center

Implementing Cisco Security Devices (CCNA/ Security)

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. The CCNA Security curriculum empha sizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.

Outline :

Module One: Security Concepts

- Common security principles
- Common security threats
- Cryptography concepts
- Describe network topologies
- Describe quality implications of a VoIP network

Module Two: Secure Access

- Secure management
- AAA concepts
- 802.1X authentication
- BYOD

Module Three: VPN

- VPN concepts
- Remote access VPN
- Site -to -site VPN

Module Four: Secure Routing and Switching

- Security on Cisco routers
- Securing routing protocols
- Securing the control plane
- Common Layer 2 attacks
- Mitigation procedures
- VLAN security

Module Five: Cisco Firewall Technologies

- Describe operational strengths and weaknesses of the different firewall technologies
- Compare stateful vs. stateless firewalls
- Implement NAT on Cisco ASA 9.x
- Implement zone -based firewall
- Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x

Module Six: IPS

- Describe IPS deployment considerations
- Describe IPS technologies

Module Seven : Content and Endpoint Security

- Describe mitigation technology for email -based threats
- Describe mitigation technology for web -based threats
- Describe mitigation technology for endpoint threats