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 emphasizes 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.

Prerequisites: Any valid CCNA Routing and Switching, or any CCIE certification can act as a prerequisite.

Recommended Training: Implementing Cisco IOS Network Security (IINS)

Exams : 640-554 IINS

Syllabus:

1.0 Common Security Threats

- 1.1 Describe common security threats

2.0 Security and Cisco Routers

- 2.1 Implement security on Cisco routers
- 2.2 Describe securing the control, data, and management plane
- 2.3 Describe CSM
- 2.4 Describe IPv4 to IPv6 transition

3.0 AAA on Cisco Devices

- 3.1 Implement AAA (authentication, authorization, and accounting)
- 3.2 Describe TACACS+
- 3.3 Describe RADIUS
- 3.4 Describe AAA

4.0 IOS ACLs

- 4.1 Describe standard, extended, and named IP IOS ACLs to filter packets
- 4.2 Describe considerations when building ACLs
- 4.3 Implement IP ACLs to mitigate threats in a network

5.0 Secure Network Management and Reporting

- 5.1 Describe secure network management
- 5.2 Implement secure network management

6.0 Common Layer 2 Attacks

- 6.1 Configure and verify network device security
- 6.2 Describe VLAN security
- 6.3 Implement VLANs and trunking
- 6.4 Implement spanning tree

7.0 Cisco Firewall Technologies

- 7.1 Describe operational strengths and weaknesses of the different firewall technologies
- 7.2 Describe stateful firewalls
- 7.3 Describe the types of NAT used in firewall technologies
- 7.4 Implement zone based policy firewall using CCP
- 7.5 Implement the Cisco Adaptive Security Appliance (ASA)
- 7.6 Implement Network Address Translation (NAT) and Port Address Translation (PAT)

8.0 Cisco IPS

- 8.1 Describe Intrusion Prevention System (IPS) deployment considerations
- 8.2 Describe IPS technologies
- 8.3 Configure Cisco IOS IPS using CCP

9.0 VPN Technologies

- 9.1 Describe the different methods used in cryptography
- 9.2 Describe VPN technologies
- 9.3 Describe the building blocks of IPSec
- 9.4 Implement an IOS IPSec site-to-site VPN with pre-shared key authentication
- 9.5 Verify VPN operations
- 9.6 Implement SSL VPN using ASA device manager