Cisco Certified Network Associate (CCNA) Security

Certification Course Agenda

Total: 32 Hours of Training

Introduction:

Cisco Certified Network Associate (CCNA) Security validates associate level knowledge and skills required to secure Cisco networks.

1. **Modern Network Security Threats**
   - Fundamental Principles of a Secure Network
   - Worms, Viruses and Trojan Horses
   - Attack Methodologies
2. **Securing Network Devices**
   - Securing Device Access and Files
   - Privilege Level and Role Based CLI
   - Monitoring Devices
   - Using Automated Features
3. **Authentication, Authorization and Accounting(AAA)**
   - Purpose of AAA
   - Configuring Local AAA
   - Configuring Serve Bases AAA
4. **Implementing Firewall Technologies**
   - Access Controls Lists
   - Firewall Technologies
   - Context Based Access Control
   - Zone Based Policy Firewall
5. **Implementing Intrusion Prevention**
   - IPS Technologies

- Implementing IPS

6. Securing the Local Area Network

- Endpoint Security Considerations
- Layer 2 Security Considerations
- Wireless , VoIP and SAN Security Considerations
- Configuring Switch Security
- SPAN and RSPAN

7. Crytography

- Cryptographic Services
- Hashes and Digital Signature
- Symmetric and Asymmetric Encryption

8. Implementing Virtual Private Networks

- VPNs
- IPSec VPN Components and Operations
- Implementing Site-to-Site IPSec VPNs
- Implementing a Remote Access VPN
- Implementing SSL and VPNs

9. Managing a Secure Network

- Secure Network Lifecycle
- Self-Defending Network
- Building a Comprehensive Security Policy