

ITNW 1049

Course Syllabus/Outline Development Form

1. NAME OF COURSE:

CISCO CCNA Security

2. NUMBER OF CLOCK HOURS:

96 hrs

3. COURSE DESCRIPTION:

This course will prepare students to take the Implementing Cisco IOS Network Security (IINS) certification exam leading to the CCNA Security certification. Topics include: securing Cisco routers, securing the network perimeter using firewall technologies, implementing endpoint and Layer 2 security, implementing secure virtual private networks, and creating a comprehensive security policy. **Prerequisites:** Cisco CCNA or equivalent skills/knowledge.

4. COURSE LEARNING OBJECTIVES:

- Develop a comprehensive network security policy to counter threats against information security
- Configure routers on the network perimeter with Cisco IOS Software security features
- Configure a Cisco IOS zone-based firewall to perform basic security operations on a network
- Configure site-to-site VPNs using Cisco IOS features
- Configure IPS on Cisco network routers
- Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic

5. RATIONALE:

Over 80% of worldwide internet traffic is controlled by CISCO routers and hubs, and those certified by CISCO in the computer networking field are in high demand.

6. REQUIRED MATERIALS:

Students will be provided with official Cisco study materials.

7. EVALUATION:

Those who participate in class discussions, score 70% or higher on the final exam, and miss no more than three class meetings will be awarded 9.6 continuing education units.

8. COURSE OUTLINE:

1. Introduction to Network Security Principles
 - Network Security Fundamentals
 - Network Attack Methodologies
 - Operations Security
 - Security Policy
 - Building Cisco Self-Defending Networks
2. Perimeter Security
 - Securing Administrative Access to Cisco Routers
 - Cisco SDM
 - Configuring AAA on a Cisco Router Using the Local Database
 - Configuring AAA on a Cisco Router to Use Cisco Secure ACS
 - Implementing Secure Management and Reporting
 - Locking Down the Router
3. Network Security Using Cisco IOS Firewalls
 - Firewall Technologies
 - Creating Static Packet Filters Using ACLs
 - Configuring Cisco IOS Zone-Based Policy Firewall
4. Site-to-Site VPNs
 - Cryptographic Services
 - Symmetric Encryption
 - Cryptographic Hashes and Digital Signatures
 - Asymmetric Encryption and PKI
 - IPsec Fundamentals
 - Building a Site-to-Site IPsec VPN
 - Configuring IPsec on a Site-to-Site VPN Using Cisco SDM
5. Network Security Using Cisco IOS IPS
 - IPS Technologies
 - Configuring Cisco IOS IPS Using Cisco SDM
6. LAN, SAN, Voice, and Endpoint Security Overview
 - Endpoint Security
 - SAN Security
 - Voice Security
 - Mitigating Layer 2 Attacks