

# Cisco Networks

## Securing Cisco Network Devices (SND)

Course:ET931

### Course Description

In this course, entry-level network security course, you'll learn basic concepts such as network security policies, network attack methods, and threat mitigation techniques, along with the Cisco security product portfolio. You will examine the most important security technologies, including hardening Cisco IOS routers and switches against attack, Layer 2 security, stateful firewalling, Intrusion Prevention Systems (IPS), and Virtual Private Networks (VPNs).

### Who should attend?

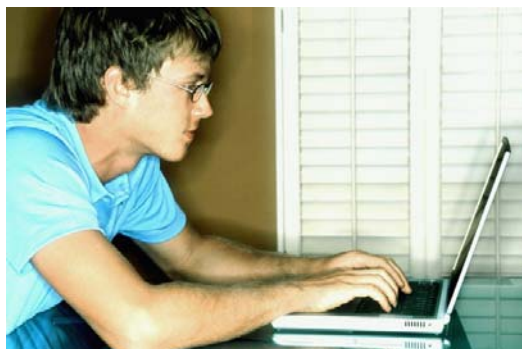
Network professionals who need to understand basic security concepts, require the basic knowledge and skills needed to deploy Cisco security, and are seeking CCSP certification, Cisco Qualified Specialist Certifications in Firewall

### Pre-requisites

- Cisco Certified Network Associate (CCNA) certification
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

### Course Objectives

- Security policies to the implementation of secure networks
- Recognize threats and vulnerabilities to networks and implement basic mitigation measures
- Various common security vulnerabilities and network attack methodologies
- Mitigation of common security vulnerabilities
- Hands-on experience with tools used by network attackers
- Hands-on experience with the security features of Cisco IOS Routers
- Hands-on experience with the security features of Cisco IOS Switches
- Discussion of specialized security devices and systems including PIX , ASA, the 4215 IPS Sensor family.
- Security Agent, and the 3000 VPN Concentrator series



### Course Outline

1. Introduction to Network Security Policies
  - Understand the Requirement for a Network Security Policy
  - Network Attack Mitigation Techniques
  - Thinking Like a Hacker
  - Designing a Secure Network Life-Cycle Model
  - Developing a Comprehensive Security Policy
  - Building Cisco Self-Defending Networks
2. Securing the Perimeter
  - Applying a Security Policy for Cisco Routers
  - Securing Administrative Access to Cisco Routers
  - Configuring AAA Functions on a Cisco Router
  - Cisco Security Device Manager (SDM)
  - Disabling Unused Cisco Router Network Services
  - Implementing Secure Management and Reporting
  - Defending the Network Perimeter with Cisco Products
3. Securing LAN and WAN Devices
  - Applying Security Policies to Network Switches
  - Mitigating Layer 2 Attacks
  - Using Cisco Catalyst Security Features
  - Securing WLANs
4. Cisco IOS Firewall Configuration
  - Firewall Technologies
  - Building Static Packet Filters with Cisco ACLs
  - Configuring a Cisco IOS Firewall with Cisco SDM
  - Defending Your Network with the Cisco Security Appliance Product Family
5. Securing Networks with Cisco IOS IPS
  - IDS and IPS
  - Configuring Cisco IOS IPS
  - Defending Your Network with the Cisco IPS Product Family
6. Building IPsec VPNs
  - IPsec Chalk Talk
  - IPsec VPNs
  - Building a Site-to-Site IPsec VPN Using the IOS CLI
  - Building a Site-to-Site IPsec VPN Using Cisco SDM
  - Building Remote-Access VPNs
  - Defending Your Network with the Cisco VPN Product Family

### Labs

- Lab 1: Network Address Translation
- Lab 2: Hacking
- Lab 3: Securing Administrative Access
- Lab 4: AAA with the Local Database
- Lab 5: SDM Security Audit
- Lab 6: Secure Management
- Lab 7: Catalyst Security Features
- Lab 8: Access Control Lists
- Lab 9: IOS Stateful Firewall
- Lab 10: IOS Intrusion Prevention Systems
- Lab 11: Site-to-Site VPN
- Lab 12: Remote-Access VPN

Register Now 02-260-3233  
<http://www.ctt-center.com>

Certifeid Technical Training Center Co.,Ltd



