



**CTREC HILTON**  
IT ACADEMY

5051 Westheimer  
Suite 500  
Houston, Texas 77056  
(713) 871-8411  
866-88-C-TREC  
Fax (713) 622-1915

Class Code: SNRS  
Number of Days: 5  
Format: Instructor-Led

## Securing Networks with Cisco Routers and Switches (SNRS ) Version 3.0

**Course Description:** Securing Networks with Cisco Routers and Switches (SNRS) v3.0 is a five-day instructor-led course presented by Cisco training partners to their end-user customers. This five-day course focuses on providing the network specialists with the knowledge and skills needed to secure Cisco IOS router and switch-based networks. Learners will be able to secure the network environment using existing Cisco IOS features, including installing and configuring Cisco IOS Classic Firewall, Cisco IOS Zone-Based Policy Firewall, user group-based firewall, Cisco IOS intrusion prevention system (IPS), authentication proxy, implementing secure tunnels using IP security (IPSec) technology, and implementing advanced switch security. This course also covers advanced virtual private network (VPN) technologies.

**Prerequisites:** To fully benefit from this course, learners should have the following prerequisite skills and knowledge:

- CCNA Security is a prerequisite for this exam/course

**Delivery Method:** Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

### Course Objectives

After completing this course, the learner will be able to meet these overall objectives:

- Implement Layer 2 security features on a network using Cisco IOS commands
- Implement Cisco Network Foundation Protection on Cisco IOS routers
- Design, install, configure and troubleshoot site-to-site VPNs using Cisco Integrated Services routers.
- Design, install, configure and troubleshoot remote-access communications using Cisco IOS security features
- Install, configure and troubleshoot url filtering, NAT and PAT, Cisco IOS Classif Firewall, Cisco IOS Zone-Based Policy Firewall, and Cisco IOS IPS on a Cisco Integrated Services router.

## Course Outline

### Module 1: Network Platform Security with Switches

- Configure Advanced Layer 2 Security
- Introducing Cisco IBNS
- Implementing Basic 802.1x Authentication
- Configure Basic 802.1x Authentication
- Configuring Advanced 802.1x Authentication and Authorization

### Module 2: Network Platform Security with Routers

- Examining the Cisco Network Foundation Protection Strategy
- Securing the Control Plane
- Securing the Management Plane
- Securing the Data Plane

### Module 3: Secure Site-to-Site Communications

- Examining VPN and IPSec Fundamentals
- Implementing IPSec VPNs with PKI
- Implementing GRE over IPSec
- Configuring High Availability VPNs and VTI
- Implementing DMVPN
- Implementing GET VPN

### Module 4: Secure Remote Access Communications

- Implementing Cisco IOS Remote Access Using Cisco Easy VPN
- Examining a Cisco IOS SSL VPN
- Configure a Cisco IOS SSL VPN

### Module 5: Threat Control and Containment

- Configuring NAT and PAT
- Configuring a Cisco IOS Classic Firewall
- Configure a Cisco IOS Classic Firewall on a Cisco Router
- Configuring a Cisco IOS Zone-Based Policy Firewall
- Configuring Cisco IOS IPS