

Cisco Networks

Securing Networks with Cisco Routers and Switches (SNRS)

Course:ET932

Course Description

This course will provide network specialists with the knowledge and skills needed to secure Cisco IOS router and switch networks. Learn to secure the network environment using existing Cisco IOS and CatOS security features, configure the three primary components of the Cisco IOS firewall feature set (context-based access control [CBAC], intrusion prevention, and authentication proxy), implement secure tunnels (VPNs) using IPSec technology, and implement basic access switch security. In addition, you will complete a security audit using functions embedded in Cisco Security Device Manager

Who should attend?

Network professionals tasked with designing and deploying Cisco Systems® security features in a Cisco IOS Software-based internetwork. This course is also recommended for anyone pursuing the certification opportunities, including Cisco Certified Security Professional (CCSP™).

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

- Configure and use Secure Shell (SSH) instead of clear text Telnet for remote command-line interface (CLI) access
- Configure command authorization and accounting instead of just user authentication
- Perform RFC 2827 filtering using unicast reverse path verification
- Perform authentication of routing updates to prevent route table poisoning
- Configure CBAC (the Cisco IOS Software feature that implements stateful packet filtering) on a three-interface router
- Explore HTTPS (instead of clear text HTTP) for authentication proxy
- Configure Advanced Encryption Standard (AES) encryption, Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES)
- Configure dynamic and static Network Address Translation (NAT) between the protected networks and the core Internet module
- Configure a fully functional security router using SDM, including NAT, firewall features, and a site-to-site VPN.
- Configure CiscoWorks to use an encrypted Secure Sockets Layer (SSL) connection for authentication, instead of clear text HTTP

Course Outline

1. Network Address Translation
 - NAT Technologies
 - Configuring NAT
 - Maintenance of NAT
 - Advanced Topics in NAT
2. Cisco Secure ACS for Windows Configuration
 - Deploying Cisco Secure Access Control Server for Windows
 - Configuring RADIUS and TACACS+ with Cisco Secure ACS for Windows
 - Configuring and Using Cisco Secure ACS for Windows
3. Configuring Cisco IOS Security Features
 - IOS Firewall CBAC (Context-Based Access Control)
 - New Features in CBAC
 - Authentication Proxy
 - IPS (Intrusion Prevention System)
4. Layer 2 Security
 - Mitigating Layer 2 Attacks
 - Cisco IBNS (Identity Based Network Services)
 - 802.1x Port-Based Authentication
 - Identifying Layer 2 Security Best Practices
5. Cisco IOS-Based Virtual Private Networks
 - Building Cisco IOS-based VPNs Using Cisco Routers and Pre-Shared Keys
 - Building Cisco IOS-based VPNs Using Cisco Routers and Certificate Authorities
 - Cisco IOS Remote Access Using Cisco Easy VPN
6. Cisco Security Device Manager (SDM)
 - Securing Cisco Routers Using Security Device Manager

Labs

- Lab 1: Network Address Translation
- Lab 2: AAA with Cisco Secure ACS
- Lab 3: Context-Based Access Control
- Lab 4: Authentication Proxy
- Lab 5: Intrusion Prevention System
- Lab 6: Switch Security
- Lab 7: 802.1x Authentication
- Lab 8: Site-to-Site IPSec Tunnels with Pre-Shared Keys
- Lab 9: Site-to-Site IPSec Tunnels with Digital Certificates
- Lab 10: Cisco Secure VPN Client
- Lab 11: SDM

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

Certifeid Technical Training Center Co.,Ltd

