

Securing Networks with Cisco Routers and Switches

Duration: 5 Days **Course Code: SNRS**

Overview:

Securing Networks with Cisco Routers and Switches (SNRS) v3.0 is a five-day, leader-led, lab-intensive course that is delivered by Cisco Learning Partners. It is aimed at providing network specialists with the knowledge and skills needed to secure Cisco IOS router and switch networks. Successful graduates will be able to secure the network environment using existing Cisco IOS features. This includes the ability to configure some of the primary components of the Cisco IOS Firewall feature set

Target Audience:

Network Designers, Administrators, Engineers and Systems engineer Network Managers, Program Managers and Project Manager

Objectives:

- Implement Layer 2 security features
- Implement the Cisco Trust and Identity Management model to control network access
- Implement command line Network Foundation Protection to protect infrastructure devices
- Implement command line Network Foundation Protection to protect infrastructure devices
- Implement secure IPsec VPNs and GRE tunnels using Cisco routers
- Install, configure, and troubleshoot Cisco IOS Firewall features, including CBAC, Cisco IOS Firewall authentication proxy, and Cisco IOS IPS on a Cisco router
- Secure tunnels using generic routing encapsulation (GRE) and IP Security (IPsec) technology
- Basic switch access security
- The Cisco Trust and Identity Management model to control network accessCommand-Line (CLI) Cisco Network Foundation Protection (NFP)

Prerequisites:

Delegates are required to meet the following prerequisites:

- CCNA or Equivalent Knowledge
- Basic knowledge of the Microsoft Windows operating system
- Basic knowledge of Cisco IOS networking and security terms and concepts.
- Familiarity with networking and security terms and concepts.
- Successful completion of ICND course.
- Successful completion of SND course.

Testing and Certification

Recommended as preparation for exam(s):

- 642-503 SNRS
This course is part of the following certifications
- Cisco Certified Security Professional (CCSP)

Follow-on-Courses:

The following courses are recommended for further study:

- SNPA – Securing Networks with PIX & ASA
- SND – Securing Cisco Network Devices
- IPS – Implementing Cisco Intrusion Prevention Systems.
- CSVPN – Cisco Secure Virtual Private Networks.

Content:

Layer 2 Security

- Examining Company ABC Unsecured
- Examining Layer 2 Attacks
- Configuring DHCP Snooping

Trust and Identity

- Implementing Identity Management
- Implementing Cisco IBNS

Cisco Network Foundation Protection

- Introducing Cisco NFP
- Securing the Control Plane
- Securing the management Plane
- Securing the Data Plane

Secured Connectivity

- Introducing IPsec
- Examining Cisco IOS VPNs
- Implementing IPsec VPNs Using Pre-Shared Keys
- Implementing IPsec VPNs Using PKI
- Configuring GRE Tunnels
- Configuring a DMVPN
- Configuring Cisco IOS SSL VPN (WebVPN)
- Configuring Cisco Easy VPN Remote Access

Adaptive Threat Defense

- Configuring Cisco IOS Firewall
- Configuring Cisco IOS Classic Firewall
- Configuring Cisco IOS Zoned-Based Policy Firewall
- Configuring Cisco IOS Firewall Authentication Proxy
- Configuring Cisco IOP IPS
- Examining Company ABC Secured

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com.eg

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo, Egypt