Global Knowledge Course Name: SNRS (Securing Networks with Cisco Routers and Switches) Code 5616

Course Overview:
Cisco Course v2.0 | Prepares you for Cisco Exam 642-503 SNRS.
In this recently updated, lab-intensive course, you'll get the knowledge and skills needed to secure Cisco IOS router and switch networks. Get in-depth training on IOS-based VPN configurations, including traditional IPSec Site-to-Site VPN, PKI/Digital Certificates for authentication, and Cisco Easy VPN Remote Access VPN. You'll also cover newer VPN technologies such as Dynamic Multipoint VPN (DMVPN) and WebVPN. Our exclusive labs extend the WebVPN experience to include the SSL VPN Client and Cisco Secure Desktop.

You will explore the three components of the IOS Firewall Feature Set: IOS Stateful Firewall, Authentication Proxy, and IOS Intrusion Prevention System, and you'll examine the classic IOS Firewall as well as the new Zone-Based policy firewall. You will explore Layer 2 security, and in our exclusive labs, you'll examine several Layer 2 attacks and learn to use IOS switch security features to mitigate those attacks.

Discover Cisco's Network Foundation Protection, including Control Plane Policing and Control Plane Protection, Management Plane Protection, Data Plane Protection, and the next generation of ACL technology, Flexible Packet Matching. You'll also work with Trust and Identity using Cisco Secure Access Control Server (ACS) to provide RADIUS services used for 802.1x network access control including dynamic VLAN assignment. Our exclusive labs include using ACS with WebVPN and Authentication Proxy.

Why Take SNRS from Global Knowledge?
We offer a unique, enhanced SNRS lab environment that allows for more practical configuration and testing scenarios. We have set ourselves apart from other Cisco training providers by enhancing our SNRS hands-on labs beyond what you'll find in a standard SNRS course. This unique solution provides an unparalleled lab infrastructure for CCSP-oriented courses and covers everything in the standard labs, plus our own exclusive material. No other training company offers a unique lab solution like ours.

Lab Enhancements Include:

- **Self-Contained Lab Environment**
  Work at your own pace in our self-contained lab environment since pods do not have to team up to complete VPN connections or test firewall and IPS features. You'll have responsibility for both sides of the VPN connection as you initiate verification traffic and witness the results.

- **Realistic Scenarios**
  Our SNRS pods include many VM images configured with various versions of Windows and Linux operating systems and with various security and attack software tools, which are placed in different security zones, providing realistic scenarios for real-world experience.
- **IOS-Firewall**
  Our IOS-FW has three interfaces supporting a DMZ, with PC systems behind each of the three interfaces, while standard labs use only a two-interface firewall with no DMZ and one PC on the inside under direct student control.
- **Network Address Translation**
  Our lab topology requires NAT between the internal networks and the simulated Internet-a fact of life in today's networks. In our labs, you'll explore NAT interaction with all other security features, and you'll learn the explicit configuration NAT often requires.
- **Hands-On Lab Environment**
  Each pod has five routers:
- **IOS-FW:** A focal point of the class. You will configure the IOS-FW as a stateful firewall, a Site-to-Site VPN termination point, a DMVPN hub, a WebVPN server, a Cisco EasyVPN server, an IOS Intrusion Prevention System sensor, and several other functions.
- **Perimeter Router:** Acts as a screening router and a demarcation point between the organization's network and the ISP.
- **Internet Router:** Simulates an Internet environment, multiple ISP routers, and other Internet-based services, such as NTP and Certificate Authority services.
- **Site1 Router:** Used for Site-to-Site and DMVPN configurations.
- **Site2 Router:** Used for DMVPN configurations.

Our SNRS pods also use a 3560 as the pod switch, which provides Layer 3 services and allows multiple internal subnets along with the configuration of standard security features, such as 802.1x and port security, and advanced security features, such as Dynamic ARP Inspection.

What You'll Learn:

- Layer 2 Security - Attack methods and techniques to mitigate the attacks
- Trust and Identity - Authentication, Authorization, and Accounting using TACACS+ and RADIUS
- 802.1x - Identity-based network access control, including dynamic VLAN assignment for end users
- Network Foundation Protection - Secure an IOS router's control plane, management plane, and data plane, and use Flexible Packet Matching
- VPN Connectivity:
- IPSec Overview

- Site-to-Site IPSec VPN using Pre-Shared Keys for Authentication
- Site-to-Site IPSec VPN using Public Key Infrastructure and Digital Certificates for Authentication
- Dynamic Multipoint VPN
- Cisco IOS SSL VPN (WebVPN)
- Easy VPN Server for Remote Access IPSec VPN
- Protect your network with Cisco IOS Classic Firewall and Cisco IOS Zone-Based Policy Firewall
- Provide identity-based access control through an IOS router using Authentication Proxy
- Defend against threats on your network using IOS Intrusion Prevention Systems

Who Needs to Attend?
Internetwork professionals who want to ensure security of their network or who seek Cisco Certified Security Professional (CCSP) certification.

Course Outline:

Layer 2 Security Features
- Examine Company ABC Unsecured
- Examine Layer 2 Attacks
- Configure DHCP Snooping

Trust and Identity
- Implement Identity Management
- Implement Cisco IBNS

Network Foundation Protection
- Network Foundation Protection Overview
- Secure the Control Plane
- Secure the Management Plane
- Secure the Data Plane

Secured Connectivity
- Introduction to IPSec
- Examine Cisco IOS VPNs
- Implement Cisco IPSec VPNs Using Pre-Shared Keys
- Implement IPSec VPNs Using PKI
- Configure GRE Tunnels
- Configure a DMVPN
- Configure Cisco IOS SSL VPN (WebVPN)
- Configure Easy VPN Remote Access

Adaptive Threat Defense

- Configure Cisco IOS Firewall
- Configure Cisco IOS Classic Firewall
- Configure Cisco IOS Zone-Based Policy Firewall
- Configure Cisco IOS Authentication Proxy
- Configure Cisco IOS IPS
- Examine Company ABC Secured