Implementing Cisco Network Security (IINS)

Duration: 5 days

Who should attend?

1. Network engineers
2. Network designers and administrators
3. Network managers
4. System engineers

Prerequisites

1. Skills and knowledge equivalent to that learned in Interconnecting Cisco Network Devices Part 1 (ICND1)
2. Working knowledge of the Windows operating system
3. Working knowledge of Cisco IOS networking and concepts

Course Objectives

1. Describe network fundamentals and build simple LANs
2. Establish Internet connectivity
3. Manage network device security
4. Expand small to medium sized networks with WAN connectivity

Course Content

Security is a top priority for virtually every organization. It is mission-critical for enterprises to secure their infrastructure from malicious attacks. This 5 day course will prepare you to design, implement, and monitor a holistic approach to network security using Cisco IOS and ASA products. You will learn through instructor discussions and hands-on labs how to perform basic tasks to secure a network using Cisco IOS devices and ASA appliance though a web-based GUI (Cisco Configuration Professional) and the CLI interfaces.

Notable differences between IINS v2.0 and v3.0
There are several notable changes in this newly updated course. Cisco Configuration Professional is not covered in IINS 3.0. All IOS examples are hands-on and done using IOS CLI. IPv6 is not covered in IINS 3.0. IPv6 is now covered in ICND1. The implementation of IPS on IOS is not covered in IINS 3.0, instead IPS is covered on the theoretical level from the perspective of FirePower technologies. Site-to-Site VPN configuration is covered on both IOS and the Cisco ASA in IINS 3.0. Also, modern malware examples are included in this course and cryptographic techniques use stronger hashing and encryption algorithms, and current version of IOS, Cisco ASA and Cisco AnyConnect are featured.