Hands-On

IINS 2.0 - Implementing Cisco IOS Network Security

CCNA-Security

Course Description

This Hands-On course will cover the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features and technologies as examples.

You will also learn about security controls of Cisco IOS devices as well as a functional introduction to the Cisco ASA adaptive security appliance.

Using instructor-led Hands-On lab exercises, this course allows you to perform basic tasks to secure a small branch office network using Cisco IOS security features, which are available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and Cisco ASA appliances and much more...

Students Will Learn

- **-Develop a comprehensive network security policy to counter threats against information security**
- **-Configure routers with Cisco IOS Software security features, including management and reporting functions**
- **-Configure IPv6 addressing, routing, and access control in Cisco network routers**
- **-Bootstrap the Cisco Adaptive Security Appliance (ASA) Firewall for use in a production network**
- **-Configure the Cisco ASA Firewall for remote access SSL VPN**
- **-Configure a Cisco IOS zone-based firewall (ZBF) to perform basic security operations on a network**
- **-Configure site-to-site VPNs using Cisco IOS features**
- **-Configure IOS IPS on Cisco network routers**
- **-Configure security features on IOS switches to mitigate various Layer 2 attacks**
- **-How a network can be compromised using freely available tools**
- **-Implement line passwords, and enable passwords and secrets**
- **-Examine Authentication, Authorization, and Accounting (AAA) concepts and features using the local database as well as Cisco Secure ACS 5.2**
- **-Run a CCP security audit and analyze the results**
- **-Configure packet filtering on the Perimeter Router**
- **-Define a virtual tunnel interface Using GRE with IPsec**
- **-And More...**

Target Audience

Anyone interested in the Hands-On skill set of CCNA-Security and or the Certification preparation of exam 640-554. Also for Network designers, Network SAN security administrators, Network, systems, and security engineers, Network and security managers

Prerequisites

ICND1 v2.0 - Interconnecting Cisco Networking Devices, Part 1

Course Outline

1. Networking Security Fundamentals

- Introducing Networking Security Concepts
- Understanding Security Policies Using a Life-Cycle Approach
- Building a Security Strategy for Borderless Networks

2. Protecting the Network Infrastructure
- Introducing Cisco Network Foundation Protection
- Protecting the Network Infrastructure Using Cisco Configuration Professional
- Securing the Management Plane on Cisco IOS Devices
- Configuring AAA on Cisco IOS Devices Using Cisco Secure ACS
- Securing the Data Plane on Cisco Catalyst Switches
- Securing the Data Plane in IPv6 Environments

3. Threat Control and Containment
- Planning a Threat Control Strategy
- Implementing Access Control Lists for Threat Mitigation
- Understanding Firewall Fundamentals
- Understanding Firewall Fundamentals
- Configuring Basic Firewall Policies on Cisco ASA Appliances
- Understanding IPS Fundamentals
- Topic 3G: Implementing Cisco IOS IPS

4. Secure Connectivity
- Understanding the Fundamentals of VPN Technologies
- Introducing Public Key Infrastructure
- Examining IPsec Fundamentals
- Implementing Site-to-Site VPNs on Cisco IOS Routers
- Implementing SSL VPNs Using Cisco ASA Appliances

Delivery Method

Instructor-Led with numerous Hands-On labs and exercises.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

5 Days