Hands-On

Implementing Adv. Cisco Unified Wireless Security

Course Description

This instructor-led course, designed to help you prepare for the CCNP wireless certification, a professional-level certification specializing in the wireless field.

The goal of the course is to prepare you to secure the wireless network from security threats via appropriate security policies and best practices, as well as ensure the proper implementation of security standards and proper configuration of security components. The IAUWS reinforces the instruction by providing you with hand-on labs to ensure thorough understanding of how to secure a network.

Students Will Learn

- **Translate organizational and regulatory security policies and enforce security compliance**
- **Integrate security on client devices**
- **Design and implement guest access services on the WLAN controller**
- **Design and integrate a wireless network with Cisco NAC Appliance**
- **Implement secure wireless connectivity services on the WLAN controller**
- **Use the internal security features on the WLAN controller and integrate the WLAN controller with advanced security platforms to isolate and mitigate security threats to the WLAN**

Target Audience

Wireless network professionals whoare required to define the security requirements for various deployment models.

Individuals wishing to attain the CCNP Wireless Certification

Prerequisites

Attendees should meet the following prerequisites CCNA in Wireless (ICND1and IUWNE)

Course Outline

Module 1: Organizational and Regulatory Security Policies

- Describing Regulatory Compliance
- Segmenting Traffic
- Configuring Administrative Security
- Managing Autonomous AP, WLAN Controller and Cisco WCS Alarms
- Identifying Security Audit Tools
- Understanding Ciscos End-to-End Security Solutions

Module 2: Secure Client Devices

- Configuring EAP Authentication
- Configuring Certificate Services
- Describing the Impact of Security on Application and Roaming
- Configuring FlexConnect Clients Authentication
- Configuring OEAP
- Configuring Cisco AnyConnect
- Implementing Access Control Lists
- Configuring Identity- Based Networking
- Troubleshooting Wireless Connectivity Connectivity Issues Related to EAP authentications

Module 3: Design and Implement Guest Access Services

- Describing Guest Access Architecture
- Configuring the WLAN to Support Guest Access
- Configuring Guest Access Accounts
- Troubleshooting Guest Access

Module 4: Design and Integrate Wireless NetworkWLAN with Cisco NAC Appliance

- Introducing the Cisco NAC Appliance Solution
- Configuring the Controller for Cisco NAC Out-of-Band Operations

Module 5: Internal and Integrated External Security Mitigation

- Mitigating Wireless Vulnerabilities
- Configuring Management Frame Protection
- Integrating the WLAN Infrastructure with IPS

Notes

Customer On-Site equipment is needed for Non-Intrusive training.

Delivery Method

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

Equipment Requirements

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

Customer On-Site equipment is needed for Non-Intrusive training.

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