IAUWS: Implementing Advanced Cisco Unified Wireless Security v2.0

Course ID#: 1575-969-ZZ-W

Hours: 35

Course Content

Course Description:

The Implementing Advanced Cisco Unified Wireless Security (IAUWS) is a 5 day ILT course, designed to help students prepare for the CCNP-Wireless certification, a professional level certification specializing in the wireless field. The goal of the IAUWS v2.0 is to provide network professional with information to prepare them 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 students with hand-on labs to ensure students thoroughly understand how to secure a wireless network.

Our IAUWS course will help you familiarize yourself with organizational and regulatory Security Policies and will teach you how to segment enterprise and quest WLAN traffic. In addition, you will review the following topics:

- Configure administration and security on a WLAN controller
- Configure administration and security on a WLAN controller using TACACS+
- Secure client devices using EAP authentication
- Configure Cisco Secure Services Client
- Design and implement guest services on a WLAN controller.
- Configure the WLAN controller for Cisco NAC
- Configure Local authentication on the WLAN controller
- Configure Management Frame Protection (MFP) on the WLAN controller
- Implement Access Control Lists (ACL) on a WLAN controller
- WLAN controller-based Intrusion Detection Signatures (IDS)
- Configure the WLAN controller to integrate with IPS and IDS appliances

Target Student:

- Wireless Network Engineer
- Mid-level Wireless Support Engineer
- Wireless Test Engineer
- Wireless Network Designer

Prerequisites:

- Cisco Certified Networking Associate – CCNA
- Cisco Certified Networking Associate Wireless– CCNA Wireless

IAUWS: Implementing Advanced Cisco Unified Wireless Security v2.0

Course ID#: 1575-969-ZZ-W

Hours: 35

Topics:

Module 1: Organizational and Regulatory Security Policies
- Regulatory Compliance
- Segmenting Traffic
- Configuring Administrative Security
- Managing WLAN Controller and Cisco WCS Alarms
- Security Audit Tools

Module 2: Secure Client Devices
- Configuring EAP Authentication
- Impact of Security on Application and Roaming
- Configuring Cisco Secure Services Client
- Troubleshooting Wireless Connectivity

Module 3: Design and Implement Guest Access Services
- Guest Access Architecture
- Configuring the WLAN to Support Guest Access
- Configuring Guest Access Accounts
- Troubleshooting Guest Access

Module 4: Design and Integrate Wireless Network with NAC
- Cisco NAC Appliance Solution
- Configuring the Controller for Cisco NAC Out-of-Band Operations

Module 5: Implement Secure Wireless Connectivity Services
- Configuring Authentication for the WLAN Infrastructure
- Configuring Management Frame Protection
- Configuring Certificate Services
- Implementing Access Control Lists
- Configuring Identity-Based Networking on the Controller Issues
- Troubleshooting Secure Wireless Connectivity

Module 6: Internal and Integrated External Security Mitigations
- Mitigating Wireless Vulnerabilities
- Using Controller-Based IDS
- Cisco's End-to-End Security Solutions
- Integrating Cisco WCS with Wireless IPS

Labs
- Implementing Advanced Cisco Unified Wireless Security
- Segmenting Traffic Identifying
- Configuring Administrative Security
- Configuring EAP Authentication on the Clients
- Configuring Cisco Secure Services Client
- Troubleshooting Wireless Connectivity
- Configure the WLAN to Support Guest Access
- Configure a Controller to use the NAC Guest Server for Authentication
- Troubleshooting Guest Access Issues
- Configuring the Controller for Cisco NAC
- Configuring Local Authentication on the WLAN Controller
- Configuring H-REAP for WAN Failure
- Configuring Management Frame Protection
- Configuring Certificate Services
- Implementing IBN
- Implementing Access Control Lists
- Troubleshooting H-REAP Security Issues
- Troubleshooting Secure Wireless Connectivity
- Using Controller-Based IDS