IAUWS (IMPLEMENTING ADVANCED CISCO UNIFIED WIRELESS SECURITY) 2.0

Objetivo

O objetivo do curso é fornecer aos profissionais de rede informações para prepará-los para proteger a rede sem fios contra ameaças de segurança através de políticas de segurança adequadas e as melhores práticas, bem como assegurar a implantação das normas de segurança e configuração adequada dos componentes de segurança. O IAUWS reforça a instrução, fornecendo labs para garantir que os alunos entendam completamente como proteger uma rede. Ao concluir este curso, o aluno será capaz de: Traduzir as políticas de segurança organizacional, regulamentar e fazer cumprir conformidades de segurança; Integrar a segurança em dispositivos dos clientes; Desenhar e implantar serviços de acesso aos convidados (Guest) na controladora; Desenhar e integrar uma rede sem fio com um Appliance Cisco NAC; Implantar serviços de conectividade sem fio segura na controladora; Use os recursos de segurança interna da controladora e a integrar com plataformas avançadas de segurança para isolar e reduzir as ameaças de segurança à WLAN.

Público Alvo

É recomendado para indivíduos que precisam saber como vender, projetar, instalar e prestar suporte às implantações de soluções WLAN.

Pré-Requisitos

Os conhecimentos e habilidades necessárias que o aluno deve possuír antes de participar deste curso: Ter participado nos treinamentos ICND1/ICND2 (CCNA R&S) e IUWNE (CCNA Wireless) ou possuír conhecimentos equivalentes.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Organizational and Regulatory Security Policies
Describing Regulatory Compliance
Segmenting Traffic
Configuring Administrative Security
Managing WLAN Controller and Cisco WCS Alarms
Identifying Security Audit Tools

Secure Client Devices

Configuring EAP Authentication
Describing the Impact of Security on Application and Client Roaming
Configuring Cisco SSC (Secure Services Client)
Troubleshooting Wireless Connectivity
Design and Implement Guest Access Services
Describing Guest Access Architecture
onfiguring the WLAN to Support Guest Access
Configuring Guest Access Accounts
Troubleshooting Guest Access

Design and Integrate a Wireless Network with Cisco NAC Appliance
Introducing the Cisco NAC Appliance Solution
Configuring the Controller for Cisco NAC Appliance for Out-of-Band Operations

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
Troubleshooting Secure Wireless Connectivity

Internal and Integrated External Security Mitigations
Mitigating Wireless Vulnerabilities
Understanding the Cisco End-to-End Security Solutions
Integrating Cisco WCS with Wireless IPS

Labs:
Organizational and Regulatory Security Policies
Segmenting Traffic
Configuring Administrative Security

Secure Client Devices
Configuring EAP Authentication on the Clients
Configuring Cisco SSC
Troubleshooting Wireless Connectivity

Design and Implement Guest Access Services
Configuring the WLAN to Support Guest Access
Configuring a Controller to use Cisco NGS for Authentication
Troubleshooting Guest Access Issues

Design and Integrate a Wireless Network with Cisco NAC Appliance
Configuring the Controller for Cisco NAC

Implement Secure Wireless Connectivity Services
Configuring Local Authentication on the WLAN Controller
Configuring H-REAP for WAN Failure

Configuring MFP
Configuring Certificate Services
Implementing ACLs
Implementing Identity Based Networking
Troubleshooting H-REAP Security Issues
Internal and Integrated External Security Mitigations
Managing Rogue Access Points
Managing IDS Signatures