WISECURE (SECURING CISCO WIRELESS ENTERPRISE NETWORKS 1.0)

Objetivo

ApÃ³s completar esse curso, o profissional vai: â¢ Determinar e descrever o processo em seguranÃ§a em redes sem fio; â¢ Desenvolver e aplicar as soluÃ§Ãµes em seguranÃ§a Cisco em uma rede sem fio; â¢ Combinar os vÃirios produtos em serviÃ§os em uma soluÃ§Ã£o robusta de seguranÃ§a em rede sem fio; â¢ Integrar a soluÃ§Ã£o para controle de acesso Cisco ISE com a rede sem fio; â¢ Implantar soluÃ§Ãµes de acesso centralizado para usuÃirios convidados em rede sem fio; â¢ Descrever e implantar soluÃ§Ãµes BYOD; â¢ Descrever e utilizar os relatÃ³rios da soluÃ§Ã£o integrada para monitoramento.

PÃºblico Alvo

Administradores de Redes Corporativas e profissisonais de revenda envolvidos na instalaÃ§Ã£o, configuraÃ§Ã£o, operaÃ§Ã£o e soluÃ§Ã£o de problemas em soluÃ§Ãµes para redes sem fio Cisco. Recomendado na preparaÃ§Ã£o de profissionais para a realizaÃ§Ã£o do exame de certificaÃ§Ã£o Cisco WISECURE (300-375), para obtenÃ§Ã£o da certificaÃ§Ã£o CCNP Wireless.

PrÃ©-Requisitos

Recomendamos que os alunos possuam os seguintes conhecimentos para uma melhor experiÃªncia e retenÃ§Ã£o de conhecimentos: â¢ Conhecimentos bÃisicos em redes locais, destacando comutaÃ§Ã£o ethernet, redes TCP/IP e roteamento. Esses conhecimentos podem ser adquiridos no curso ICND1; â¢ Conhecimentos bÃisicos em redes sem fio, destacando soluÃ§Ãµes Wi-Fi 802.11 em redes locais, seus protocolos, suas especificaÃ§Ãµes e melhores prÃiticas de implantaÃ§Ã£o. Esses conhecimentos podem ser adquiridos no curso WIFUND; â¢ Conhecimento bÃisicos e experiÃªncia na utilizaÃ§Ã£o dos produtos Cisco Prime Infrastructure e MSE (Mobility Identity Engine), Cisco ISE (Identity Services Engine); â¢ Conhecimentos bÃiscos em seguranÃ§a.

Carga HorÃiria

40 horas (5 dias).

ConteÃºdo ProgramÃitico

Course Introduction

Security Areas in the Wi-Fi Design

Security Challenges for IT Organizations
Device Support

Security and Usage Policy
Protecting Corporate Data
Modern Wi-Fi Security Concerns
Advantages of a Comprehensive BYOD Approach
AAA Solution
Compliance Regulations
Trends in Regulatory Compliance
Components of a Comprehensive Security Policy
Technical and End-User Policies
Standards, Guidelines, and Procedures
Security Policy Responsibilities
Security Awareness

Security Approaches in Wi-Fi Designs

Basic Security Assumptions
Basic Security Requirements
Risk: Motivation Meets Opportunity
Communication Security Challenges: Mobility, Emerging Threats, and Compliance
Policy Enforcement for Users and Devices
Cisco Lightweight Access Points
Wireless Controller
Cisco ISE
Cisco Prime Infrastructure
Guest Access Needs
Categorizing Wireless Vulnerabilities
Rogue APs and Clients
Denial of Service
Over-the-Air Attacks
What Is Defense in Depth?
802.1X and EAP
Protection of Management Frames
Functions in a wIPS Deployment
Authentication, Authorization & Accounting
Change of Authorization
RADIUS
TACACS+

Endpoint and Client Standards and Features

Authenticating Devices vs. Users
Open Authentication
Encryption
Symmetric and Asymmetric Encryption
Individual Keys
Common Keys
Digital Signature
RSA Digital Signatures

Trusted Third Party
Certificates X.509 Version 3
PKI Terminology and Components
Wireless IDS
IEEE 802.1X over Wireless
802.1X, EAP, and the AAA Relationship
EAP-TLS Authentication
EAP-PEAP Authentication
EAP-FAST Authentication
Local EAP Authentication
WPA, WPA2 and IEEE 802.11i
Configure WPA, WPA2 and EAP in a Wi-Fi environment
External RADIUS Server
IEEE 802.11k Radio Resource Management
IEEE 802.11r Fast BSS Transition

Cisco Network Security Architecture

Security Challenges for IT Organizations
Cisco ISE Architecture, Components, and Licensing
Cisco ISE Nodes, Personas, and Roles
Network Access Device
Cisco ISE Licensing
Cisco ISE Appliances
VM Requirements
Installing Cisco ISE

Profiles and Policies

End Device Analysis with Cisco ISE Profiling
Cisco ISE Profiler
Profiling Policies
Cisco ISE Probes
Device Sensor
Create Policies in Cisco ISE
Considerations for Defining Policy Elements
Cisco ISE Workflow
Authentication in Cisco ISE
Rule-Based Authentication Policies
Authentication Policy
Identity Groups
Authorization Profiles
Change of Authorization
Policy Sets

Guest Access

Wireless Guest DMZ Networks

Defining the Guest User
Guest User Role-Based Policies
Guest User Databases
Guest Provisioning Services
Comparison of Central versus Local WebAuth
Central Web Authentication
Cisco ISE URL Redirection
Requirements for Configuring CWA
Wireless CWA Configuration
Cisco CMX Visitor Connect

Secure BYOD

Configure BYOD
Advantages of Cisco BYOD Solution
Cisco Solution Components
Onboarding
Device Authentication for BYOD
Cisco ISE Authentication and Authorization Policies Supporting BYOD
Single or Dual SSID in BYOD
Client Provisioning
CWA and IEEE 802.1X Use Cases
My Devices Portal
Cisco ISE Device Profiling
BYOD Profiling with CoA
Cisco ISE and Cisco Prime Infrastructure Integration
Cisco ISE and Cisco Prime Infrastructure Reporting
Device 360º View Wireless Controller
Cisco Prime Infrastructure Alarms and Events
Cisco Prime Infrastructure Client Monitoring Dashboard
Cisco Prime Infrastructure Clients and Users
Cisco Prime Infrastructure: Client Properties
Cisco ISE Live Authentication
Cisco WLC Authorization Diagnosis

Defining Endpoint and Client Standards and Features

Infrastructure MFP
Infrastructure Mode
Client MFP
Client and Infrastructure Mode
IEEE 802.11w Protection
MFP vs. IEEE 802.11w
Using Identity-Based Networking
Authorization Options for Users and Devices
VLANs and ACLs
Downloadable ACL vs. Airspace ACL
Preauthentication and Postauthentication ACLs

External Authentication Server
Configure SMNP in the Wi-Fi Environment
Cisco Prime Infrastructure Configure Controllers

Defining Wi-FI Access Control Standards and Features

ACLs and Firewall Functionality
ACL Functionality and Limits
Firewalls
VPN Firewall
FlexConnect ACLs
Autonomous AP
Cisco WLC Configure a New ACL
ACL Types

Defining Threat and Interference Mitigation Approaches in Wi-Fi

Rogue Access Points and Clients
Hacker APs
Denial of Service
Over-the-Air Attacks
Interference
Policy Enforcement
Rogue Detection
Rogue Classification
Rogue States
Cisco WLC Monitoring the Logs
Controller-Based IDS
wIPS Features
Cisco IPS Integration
wIPS Alarm Flow
wIPS AP Placement
Configure Cisco Prime Infrastructure for wIPS
Add a Cisco MSE to Cisco Prime Infrastructure
Install wIPS License Files
Synchronize Cisco Prime Infrastructure and Cisco MSE
Configure Cisco Prime Infrastructure for wIPS
Enable the Radios
Configure Rogue Detection and Mitigation in the Wi-Fi Environment
Rogue Detector AP
Enable Rogue Detector Mode
Rogue Location Discovery Protocol
Configure Spectrum Expert
Cisco CleanAir
Reports

Discovery labs

Discovery 1: Overview of Cisco ISE
Discovery 2: Implementing SNMP v3
Discovery 3: Configure and Verify Cisco MFP
Discovery 4: Rogue AP Monitoring and Rules

Labs:
Lab 1: Configure WPA2 Access
Lab 2: Configure 802.1X Access
Lab 3: Configure RADIUS Integration
Lab 4: Configure a Basic Access Policy
Lab 5: Configure a Contractor2 Authentication Policy
Lab 6: Configure Hotspot Guest Access
Lab 7: CWA and Self-Registered Guest Operations
Lab 8: Configure Secure Administrative Access
Lab 9: Configure a Basic Authentication Policy for an AP
Lab 10: Implement Profiling
Lab 11: Profiling and Device Onboarding
Lab 12: Cisco ISE Profiling Reports
Lab 13: Guest Reports
Lab 14: Live Logs and Client 360° View
Lab 15: Security Report Operations
Lab 16: Use System Security Verification Tools