



Implementing Advanced Cisco Unified Wireless Security

Objectifs

Après avoir suivi le cours, les stagiaires seront capables de :

- Comprendre les politiques de sécurité et renforcer la compatibilité de la sécurité.
- Sécuriser les équipements des clients
- Concevoir et implémenter un service d'accès aux invités sur un contrôleur WLAN
- Concevoir et intégrer un réseau sans-fil avec un Appliance NAC de Cisco
- Mettre en place un service de connexion sécurisé sans-fil sur un contrôleur WLAN
- Utiliser les fonctions intégrées de sécurité d'un contrôleur WLAN et les intégrer avec des plateformes de sécurité avancées pour isoler et gérer les failles de sécurité d'un réseau WLAN.

IAUWS

3250€ HT
Version : 1.0
5 jours

A qui s'adresse ce cours ?

- Aux ingénieurs de réseau sans fil Cisco®
- Aux ingénieurs de Test de réseau sans fil Cisco®
- Aux administrateurs de réseaux sans fil Cisco®
- Aux managers de réseaux sans fil Cisco®
- Aux ingénieurs wifi de niveau intermédiaire Cisco®
- Aux managers de projet Cisco®
- Aux commerciaux Cisco®

Pré-requis

- Avoir suivi le cours *Implementing Cisco Unified Wireless Networking Essentials* (IUWNE)
- Avoir suivi le cours *Interconnecting Cisco Networking Devices Part 1* (ICND1)
- Avoir suivi le cours *Interconnecting Cisco Networking Devices Part 2* (ICND2)

Contenu du stage

1. Organizational and Regulatory Security Policies

- 1.1. Description des compatibilités liées aux domaines de régulation
- 1.2. Segmenter le trafic
- 1.3. Configuration de la sécurité administrative
- 1.4. Gérer un contrôleur WLAN et les alarmes du Cisco WCS
- 1.5. Identifier les outils d'audit de sécurité

2. Sécuriser les équipements des clients

- 2.1. Configurer un système d'authentification EAP
- 2.2. Description des impacts liés à la sécurité avec les applications et le roaming des clients
- 2.3. Configurer un Cisco SSC
- 2.4. Dépanner des connexions sans-fils

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.



3. Concevoir et intégrer un service d'accès invités

- 3.1. Décrire l'architecture d'un accès invité
- 3.2. Configurer des accès invités sur un WLAN
- 3.3. Configurer les comptes invités
- 3.4. Dépanner des accès invités

4. Concevoir et intégrer un réseau sans-fil avec un Appliance NAC de Cisco

- 4.1. Introduction de l'appliance NAC de Cisco
- 4.2. Configurer un controller avec un appliance NAC pour les opérations de type Out-of-Band

5. Mettre en œuvre un service de connexion sans-fil sécurisé

- 5.1. Configurer un système d'authentification sur une infrastructure WLAN
- 5.2. Configurer la gestion du Management Frame Protection
- 5.3. Configurer les services de certificats
- 5.4. Mettre en place des ACLs
- 5.5. Dépanner des connexions sans-fil sécurisées

6. Gestion de la sécurité en interne ou avec des équipements externes intégrés

- 6.1. Gérer les vulnérabilités liées au sans-fil
- 6.2. Comprendre les solutions Cisco de filtrage d'URL pour l'utilisateur final
- 6.3. Intégrer le Cisco WCS avec les sondes Wireless IPS

Déroulement du stage

	Jour 1	Jour 2	Jour 3	Jour 4	Jour 5
MATIN	Introduction Describing Regulatory Compliance Segmenting Traffic Lab 1-1: Segmenting Traffic	Configuring EAP Authentication (Cont.) Lab 2-1: Configuring EAP Authentication on the Clients Describing the Impact of Security on Application and Client Roaming Configuring Cisco SSC Lab 2-2: Configuring Cisco SSC	Lab 3-2: Configuring a Controller to use Cisco NGS for Authentication Troubleshooting Guest Access Lab 3-3: Troubleshooting Guest Access Issues Lab 3-3: Troubleshooting Guest Access Issues (Cont.) Module Summary and Self-Check Introducing the Cisco NAC Appliance Solution	Configuring Management Frame Protection Lab 5-3: Configuring MFP Configuring Certificate Services Lab 5-4: Configuring Certificate Services Implementing ACLs	Mitigating Wireless Vulnerabilities (Cont.) Lab 6-1: Managing Rogue Access Points Lab 6-2: Managing IDS Signatures
APRES-MIDI	Configuring Administrative Security Lab 1-2: Configuring Administrative Security	Troubleshooting Wireless Connectivity Lab 2-3: Troubleshooting Wireless Connectivity	Configuring the Controller for Cisco NAC Out-of-Band Operations Lab 4-1: Configuring the	Lab 5-5: Implementing Access Control Lists Implementing Identity Based Networking	

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.



Managing WLAN Controller and Cisco WCS Alarms Identifying Security Audit Tools Module Summary and Self-Check Configuring EAP Authentication	Module Summary and Self-Check Describing Guest Access Architecture Configuring the WLAN to Support Guest Access Lab 3-1: Configuring the WLAN to Support Guest Access Configuring Guest Access Accounts	Controller for Cisco NAC Module Summary and Self-Check Configuring Authentication for the WLAN Infrastructure Lab 5-1: Configuring Local Authentication on the WLAN Controller Lab 5-2: Configuring H-REAP for WAN Failure	Lab 5-6: Implementing Identity Based Networking Troubleshooting Secure Wireless Connectivity Lab 5-7: Troubleshooting H-REAP Security Issues Module Summary and Self Check Mitigating Wireless Vulnerabilities	Understanding the Cisco End-to-End Security Solutions (Cont.) Integrating Cisco WCS and Wireless IPS Module Summary and Self-Check
--	---	--	--	--

Laboratoires pratiques

- Topologie du Lab
- Exigences Matérielles et Logiciels
- Configuration d'un Poste de Travail
- Configuration des équipements du Lab
- Installation general du Lab
- Lab 1-1: Segmenting Traffic
- Lab 1-2: Configurer l'administration de sécurité
- Lab 2-1: Configuring EAP Authentication on the Clients
- Lab 2-2: Configurer un Cisco SSC
- Lab 2-3: Dépanner des connexions sans-fils
- Lab 3-1: Configuring the WLAN to Support Guest Access
- Lab 3-2: Configuring a Controller to use Cisco NGS for Authentication
- Lab 3-3: Dépanner des accès invités Lab 4-1: Configuration du contrôleur pour le NAC Cisco
- Lab 5-1: Configuring Local Authentication on the WLAN Controller
- Lab 5-2: Configurer un H-REAP dans le cas d'une erreur
- Lab 5-3: Configurer le MFP Configuring MFP
- Lab 5-4: Configuring Certificate Services
- Lab 5-5: Mettre en oeuvre une ACLs
- Lab 5-6: Implementing Identity Based Networking
- Lab 5-7: Troubleshooting H-REAP Security Issues
- Lab 6-1: Managing Rogue Access Points
- Lab 6-2: Gestion des signatures IDS
- Solutions des activités du lab Lab Activity Solutions
- Teardown and Restoration

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.