Guide de configuration et de déploiement de WIPS ELM adaptatif

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Conventions](#)
[Flux d'alarmes wIPS ELM](#)
[Considérations de déploiement pour ELM](#)
[ELM et MM dédié](#)
[Performances sur canal et hors canal](#)
[ELM sur les liaisons WAN](#)
[Intégration de CleanAir](#)
[Caractéristiques et avantages d'ELM](#)
[Licences ELM](#)
[Configuration d'ELM avec WCS](#)
[Configuration à partir du WLC](#)
[Attaques détectées dans ELM](#)
[Dépannage d'ELM](#)
[Informations connexes](#)

Introduction

La solution Cisco Adaptive Wireless Intrusion Prevention System (wIPS) ajoute la fonctionnalité ELM (Enhanced Local Mode), permettant aux administrateurs d'utiliser leurs points d'accès déployés pour fournir une protection complète sans avoir besoin d'un réseau de superposition séparé (Figure 1). Avant ELM et dans le déploiement wIPS adaptatif traditionnel, des points d'accès en mode surveillance (MM) dédiés sont requis pour répondre aux besoins de conformité PCI ou pour assurer une protection contre les accès de sécurité non autorisés, la pénétration et les attaques (Figure 2). ELM présente une offre comparable qui soulage la mise en œuvre d'un système de sécurité sans fil tout en diminuant les dépenses en capital et les coûts d'exploitation. Ce document se concentre uniquement sur ELM et ne modifie pas les avantages existants du déploiement wIPS avec les points d'accès MM.

Figure 1 - Déploiement amélioré des points d'accès en mode local

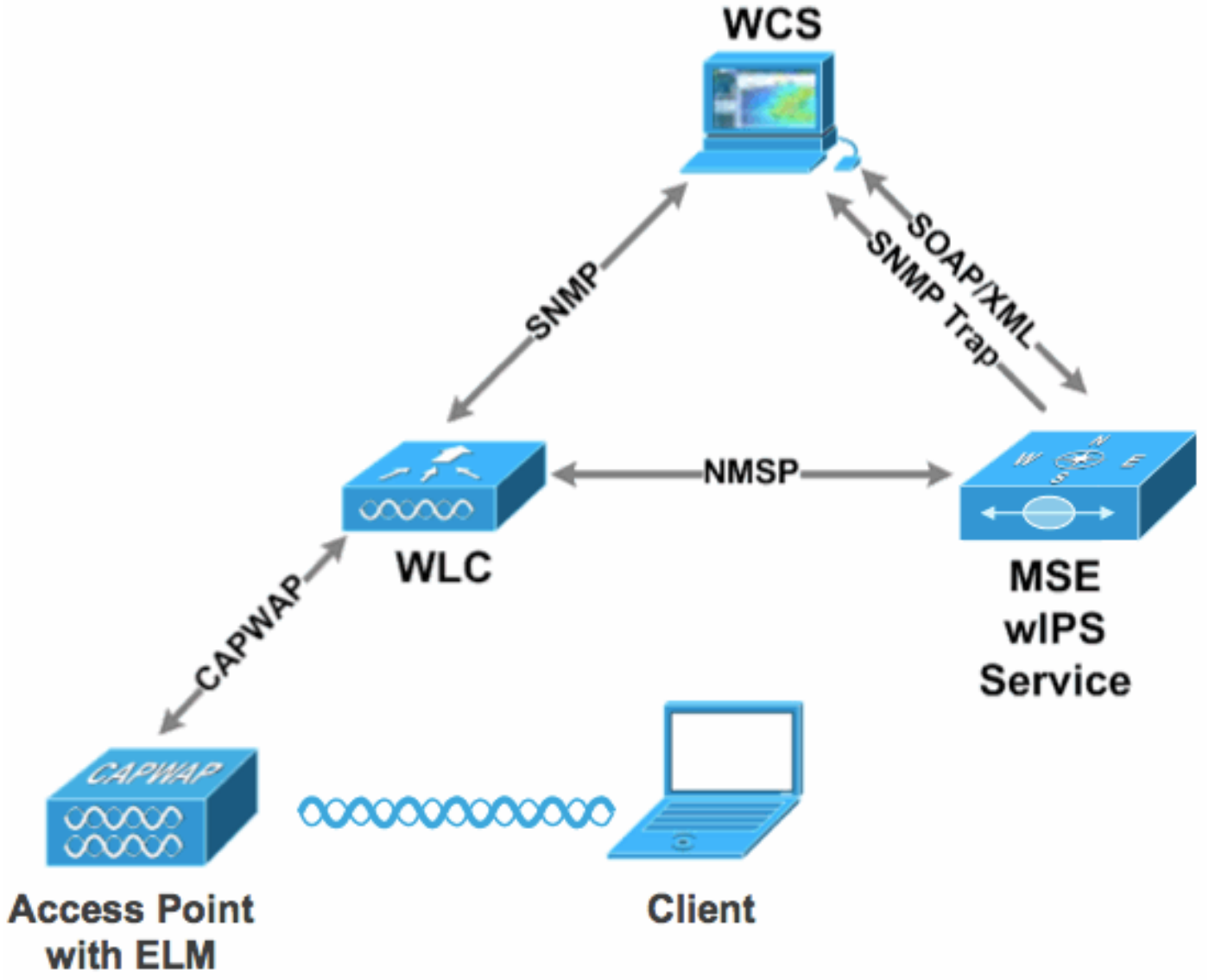
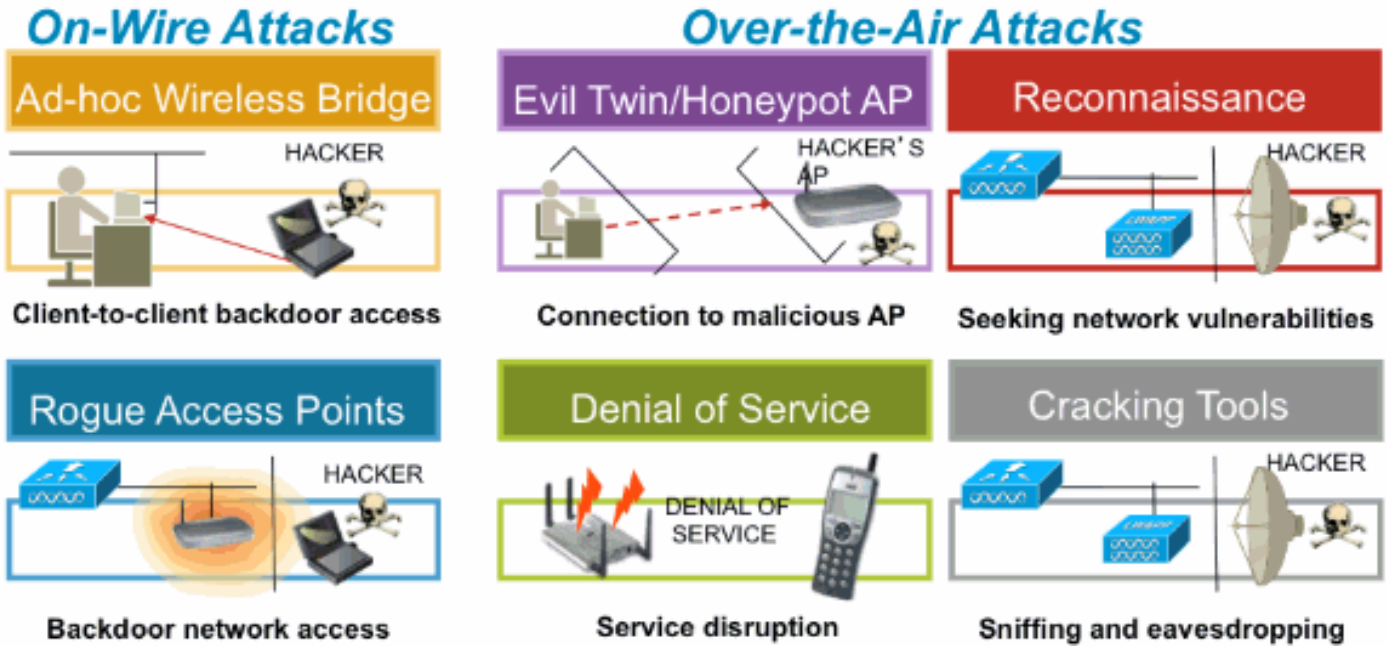


Figure 2 : principales menaces pour la sécurité sans fil



Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Composants requis d'ELM et versions de code minimales

- Contrôleur LAN sans fil (WLC) - Version 7.0.116.xx ou ultérieure
- AP - Version 7.0.116.xx ou ultérieure
- Wireless Control System (WCS) - Version 7.0.172.xx ou ultérieure
- Mobility Services Engine - Version 7.0.201.xx ou ultérieure

Prise en charge des plates-formes WLC

ELM est pris en charge sur les plates-formes WLC5508, WLC4400, WLC 2106, WLC2504, WiSM-1 et WiSM-2WLC.

Prise en charge des AP

ELM est pris en charge sur les points d'accès 11n, notamment 3500, 1250, 1260, 1040 et 1140.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

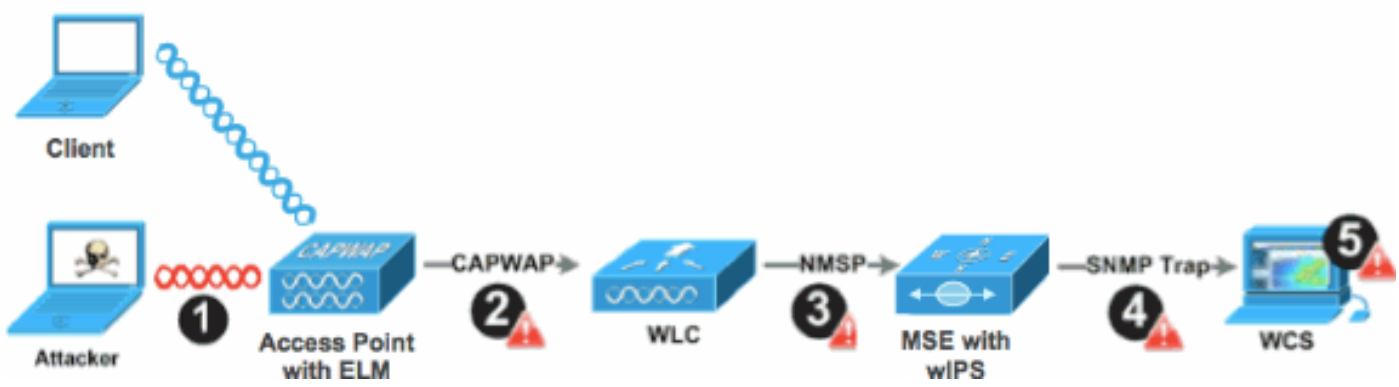
Flux d'alarmes wIPS ELM

Les attaques ne sont pertinentes que lorsqu'elles se produisent sur des points d'accès d'infrastructure approuvés. Les points d'accès ELM détectent et communiquent avec le contrôleur et établissent une corrélation avec le MSE pour le reporting avec la gestion WCS. La Figure 3 présente le flux d'alarmes du point de vue de l'administrateur :

1. Attaque lancée contre un périphérique d'infrastructure (point d'accès « approuvé »)
2. Détecté sur l'AP ELM communiqué via CAPWAP au WLC
3. Transmis de manière transparente à MSE via NMSP

4. Connecté à la base de données wIPS sur MSE Envoyé à WCS via une interruption SNMP
5. Affiché au WCS

Figure 3 - Détection des menaces et flux d'alarmes



Considérations de déploiement pour ELM

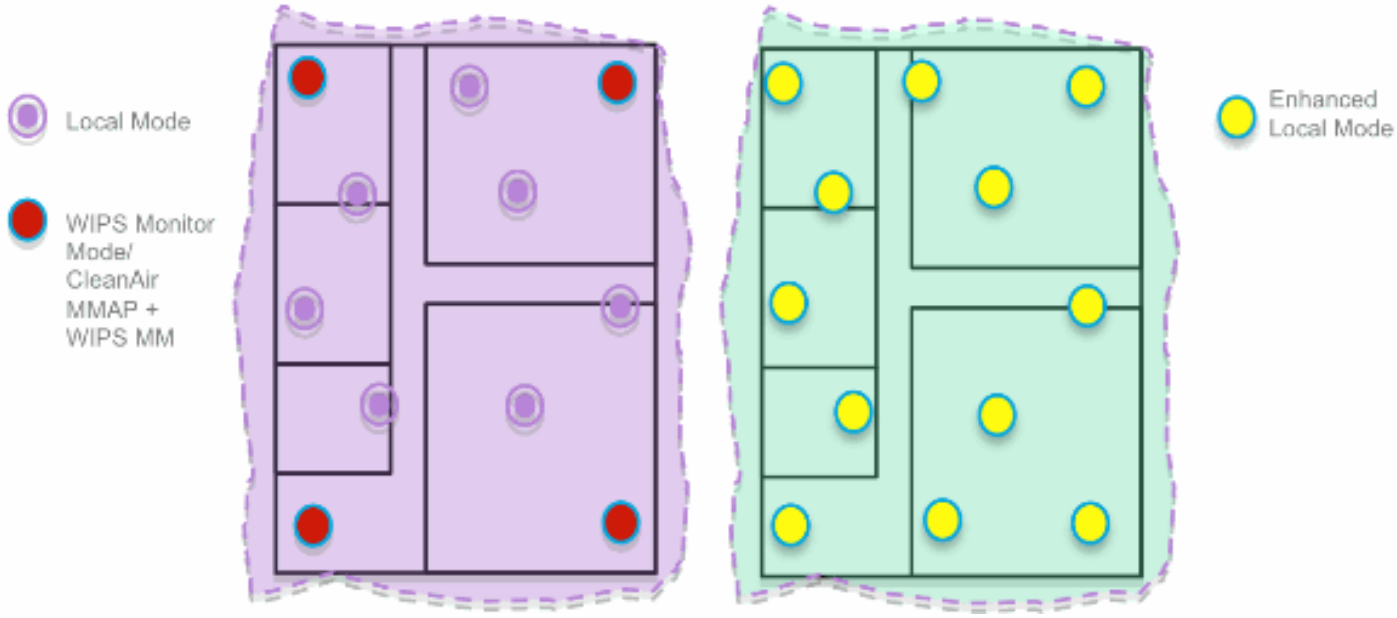
Cisco recommande qu'en activant ELM sur chaque point d'accès du réseau, vous répondiez à la plupart des besoins des clients en matière de sécurité lorsqu'une superposition de réseau et/ou des coûts sont pris en compte. La fonction principale d'ELM fonctionne efficacement pour les attaques sur canal, sans compromettre les performances sur les clients et services de données, voix et vidéo.

ELM et MM dédié

La Figure 4 présente un contraste général entre les déploiements standard des points d'accès wIPS MM et ELM. En résumé, la plage de couverture type pour les deux modes suggère :

- Le point d'accès wIPS MM dédié couvre généralement entre 1 500 et 35 000 pieds carrés
- Le point d'accès client couvre généralement entre 3 000 et 5 000 pieds carrés

Figure 4 - Recouvrement de MM par rapport à tous les points d'accès ELM



Dans le déploiement wIPS adaptatif traditionnel, Cisco recommande un rapport de 1 MM AP sur 5 points d'accès en mode local, qui peut également varier en fonction de la conception du réseau et des conseils d'experts pour une meilleure couverture. En considérant ELM, l'administrateur active simplement la fonctionnalité logicielle ELM pour tous les points d'accès existants, ajoutant efficacement les opérations MwIPS au point d'accès en mode de service de données local tout en maintenant les performances.

Performances sur canal et hors canal

Un point d'accès MM utilise 100 % du temps de la radio pour analyser tous les canaux, car il ne sert aucun client WLAN. La principale fonctionnalité d'ELM fonctionne efficacement pour les attaques sur canal, sans compromettre les performances sur les clients et services de données, voix et vidéo. La principale différence réside dans le fait que le mode local fait varier l'analyse hors canal ; en fonction de l'activité, l'analyse hors canal fournit un temps d'arrêt minimal pour rassembler suffisamment d'informations disponibles pour classer et déterminer l'attaque. Un exemple peut être avec des clients vocaux qui sont associés et où l'analyse RRM d'AP est différée jusqu'à ce que le client vocal soit désassocié pour s'assurer que le service n'est pas affecté. Pour cette considération, la détection ELM pendant hors canal est considérée comme le meilleur effort. Les points d'accès ELM voisins fonctionnant sur tous les canaux, pays ou DCA augmentent l'efficacité, d'où la recommandation d'activer ELM sur chaque point d'accès en mode local pour une couverture de protection maximale. Si l'analyse dédiée est requise sur tous les canaux à temps plein, il est recommandé de déployer des points d'accès MM.

Ces points examinent les différences entre le mode local et les points d'accès MM :

- Point d'accès en mode local : permet aux clients WLAN d'effectuer un découpage temporel de l'analyse hors canal, écoute 50 ms sur chaque canal et offre une analyse configurable pour tous les canaux/pays/DCA.
- Point d'accès en mode surveillance : ne sert pas les clients WLAN, dédiés à l'analyse uniquement, écoute 1,2 s sur chaque canal et analyse tous les canaux.

ELM sur les liaisons WAN

Cisco a fait de gros efforts pour optimiser les fonctionnalités dans des scénarios difficiles, tels que le déploiement de points d'accès ELM sur des liaisons WAN à faible bande passante. La fonctionnalité ELM implique un pré-traitement pour déterminer les signatures d'attaque au niveau du point d'accès et est optimisée pour fonctionner sur des liaisons lentes. En tant que meilleures pratiques, il est recommandé de tester et de mesurer la ligne de base pour valider les performances avec ELM sur WAN.

Intégration de CleanAir

La fonctionnalité ELM complète les opérations CleanAir avec des performances et des avantages similaires au déploiement des points d'accès MM avec ces avantages existants sensibles au spectre CleanAir :

- Intelligence RF dédiée au niveau du silicium
- Reconnaissance du spectre, autoréparation et auto-optimisation
- Détection et réduction des menaces et des interférences sur les canaux non standard
- Détection non Wi-Fi (Bluetooth, micro-ondes, téléphones sans fil, etc.)
- Détecter et localiser les attaques DOS de la couche RF, telles que les brouilleurs RF

Caractéristiques et avantages d'ELM

- Analyse wIPS adaptative dans des points d'accès locaux et H-REAP de service de données
- Protection sans nécessiter de réseau de recouvrement séparé
- Disponible en téléchargement logiciel gratuit pour les clients wIPS existants
- Prise en charge de la conformité PCI pour les réseaux locaux sans fil
- Détection complète des attaques 802.11 et non 802.11
- Ajoute des fonctionnalités d'analyse et de reporting
- Intégration à la gestion CUWM et WLAN existante
- Flexibilité pour définir des points d'accès MM intégrés ou dédiés
- Le prétraitement au niveau des points d’accès réduit la liaison de données (fonctionne sur des liaisons à très faible bande passante)
- Faible impact sur les données de service

Licences ELM

ELM wIPS ajoute une nouvelle licence à la commande :

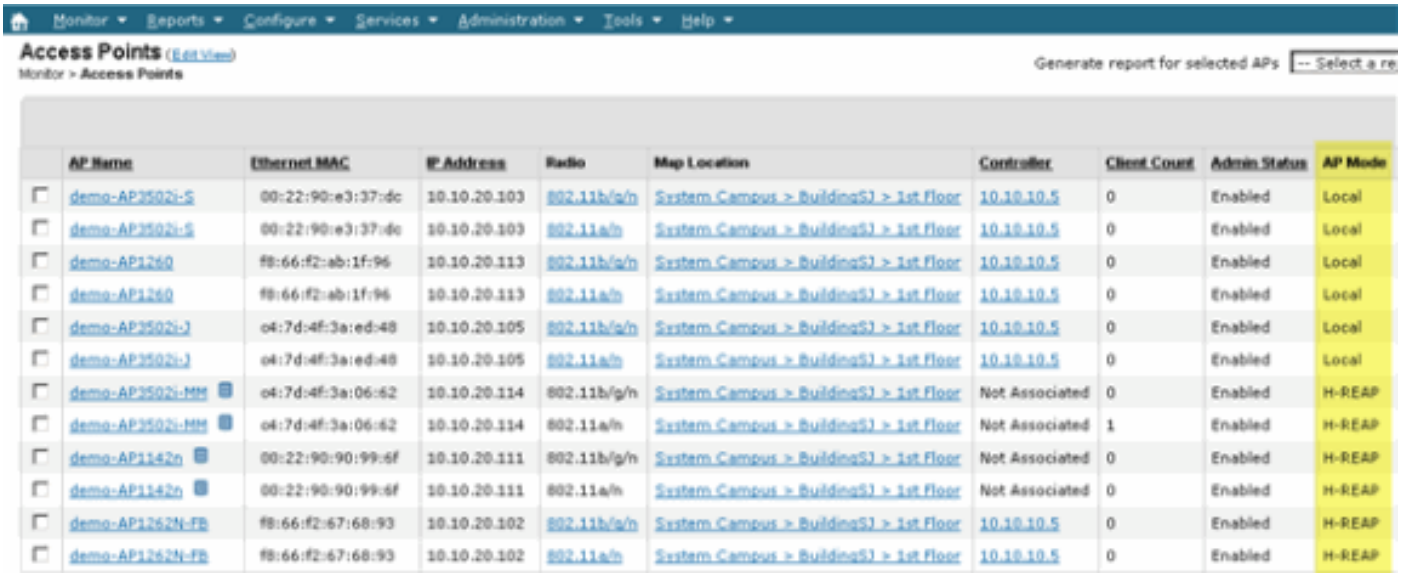
- AIR-LM-WIPS-xx - Licence Cisco ELM wIPS
- AIR-WIPS-AP-xx - Licence Cisco Wireless wIPS

Notes de licence ELM supplémentaires :

- Si des références de licence de point d'accès wIPS MM sont déjà installées, ces licences peuvent également être utilisées pour les points d'accès ELM.
- Les licences wIPS et ELM sont prises en compte dans les limites de licence de plate-forme pour le moteur wIPS ; 2 000 points d'accès sur 3310 et 3 000 points d'accès sur 335x, respectivement.
- La licence d'évaluation inclura 10 points d'accès pour wIPS et 10 pour ELM pendant une période pouvant atteindre 60 jours. Avant ELM, la licence d'évaluation autorisait jusqu'à 20 points d'accès wIPS MM. La configuration minimale requise pour les versions logicielles prenant en charge ELM doit être respectée.

Configuration d'ELM avec WCS

Figure 5 - Utilisation de WCS pour configurer ELM



AP Name	Ethernet MAC	IP Address	Radio	Map Location	Controller	Client Count	Admin Status	AP Mode
demo-AP3502i-S	00:22:90:e3:37:dc	10.10.20.103	802.11b/g/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-S	00:22:90:e3:37:dc	10.10.20.103	802.11a/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP1260	f8:66:f2:ab:1f:96	10.10.20.113	802.11b/g/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP1260	f8:66:f2:ab:1f:96	10.10.20.113	802.11a/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-J	o4:7d:4f:3a:ed:48	10.10.20.105	802.11b/g/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-J	o4:7d:4f:3a:ed:48	10.10.20.105	802.11a/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-MM	o4:7d:4f:3a:06:62	10.10.20.114	802.11b/g/n	System Campus > Building5 > 1st Floor	Not Associated	0	Enabled	H-REAP
demo-AP3502i-MM	o4:7d:4f:3a:06:62	10.10.20.114	802.11a/n	System Campus > Building5 > 1st Floor	Not Associated	1	Enabled	H-REAP
demo-AP1142n	00:22:90:90:99:6f	10.10.20.111	802.11b/g/n	System Campus > Building5 > 1st Floor	Not Associated	0	Enabled	H-REAP
demo-AP1142n	00:22:90:90:99:6f	10.10.20.111	802.11a/n	System Campus > Building5 > 1st Floor	Not Associated	0	Enabled	H-REAP
demo-AP1262N-FB	f8:66:f2:67:68:93	10.10.20.102	802.11b/g/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	H-REAP
demo-AP1262N-FB	f8:66:f2:67:68:93	10.10.20.102	802.11a/n	System Campus > Building5 > 1st Floor	10.10.10.5	0	Enabled	H-REAP

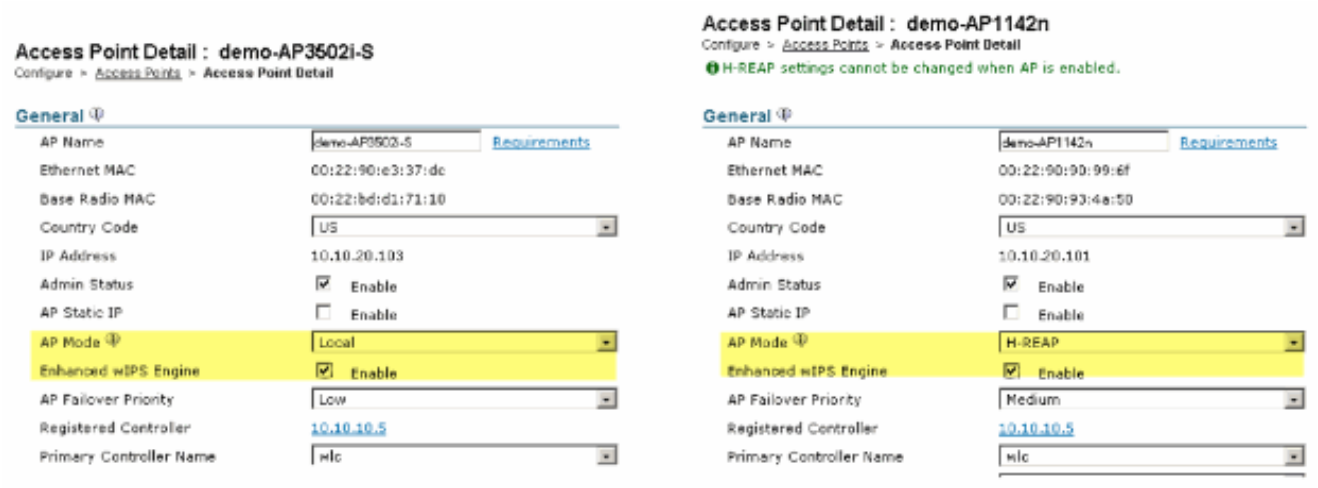
1. À partir de WCS, désactivez les radios 802.11b/g et 802.11a du point d'accès avant d'activer le « moteur wIPS amélioré ».

   Remarque : tous les clients associés sont déconnectés et ne se connectent pas tant que les radios ne sont pas activées.

2. Configurez un point d'accès ou utilisez un modèle de configuration WCS pour plusieurs

points d'accès légers. Voir la figure 6.

Figure 6 : activation du sous-mode Enhanced wIPS Engine (ELM)



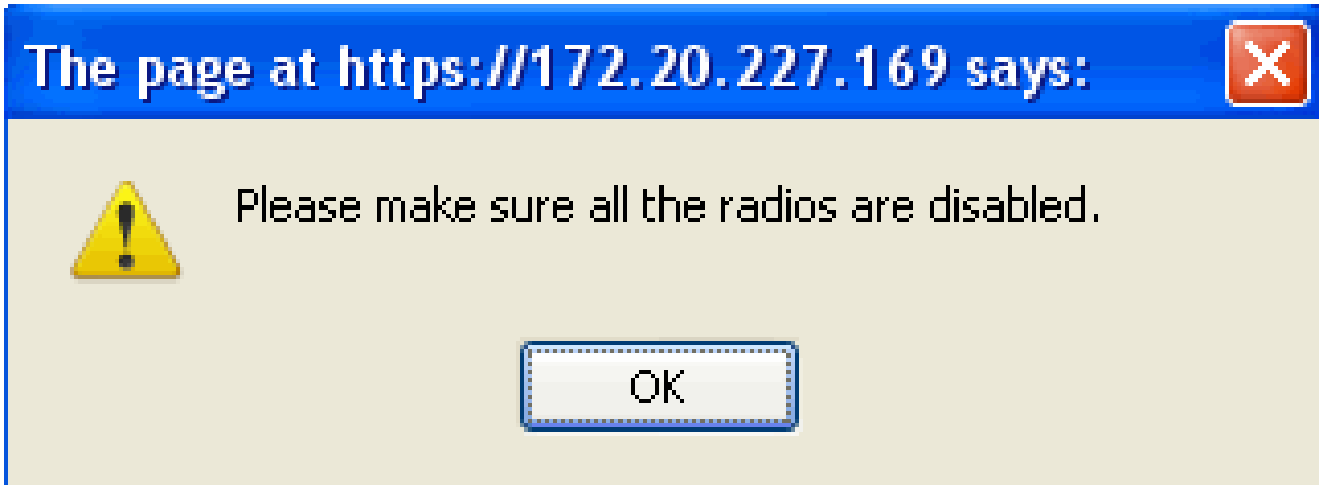
3. Choisissez Enhanced wIPS Engine, puis cliquez sur Save.

    a. L'activation du moteur wIPS amélioré n'entraînera pas le redémarrage du point d'accès.

    b. H-REAP est pris en charge ; activez-le de la même manière que pour le mode local AP.

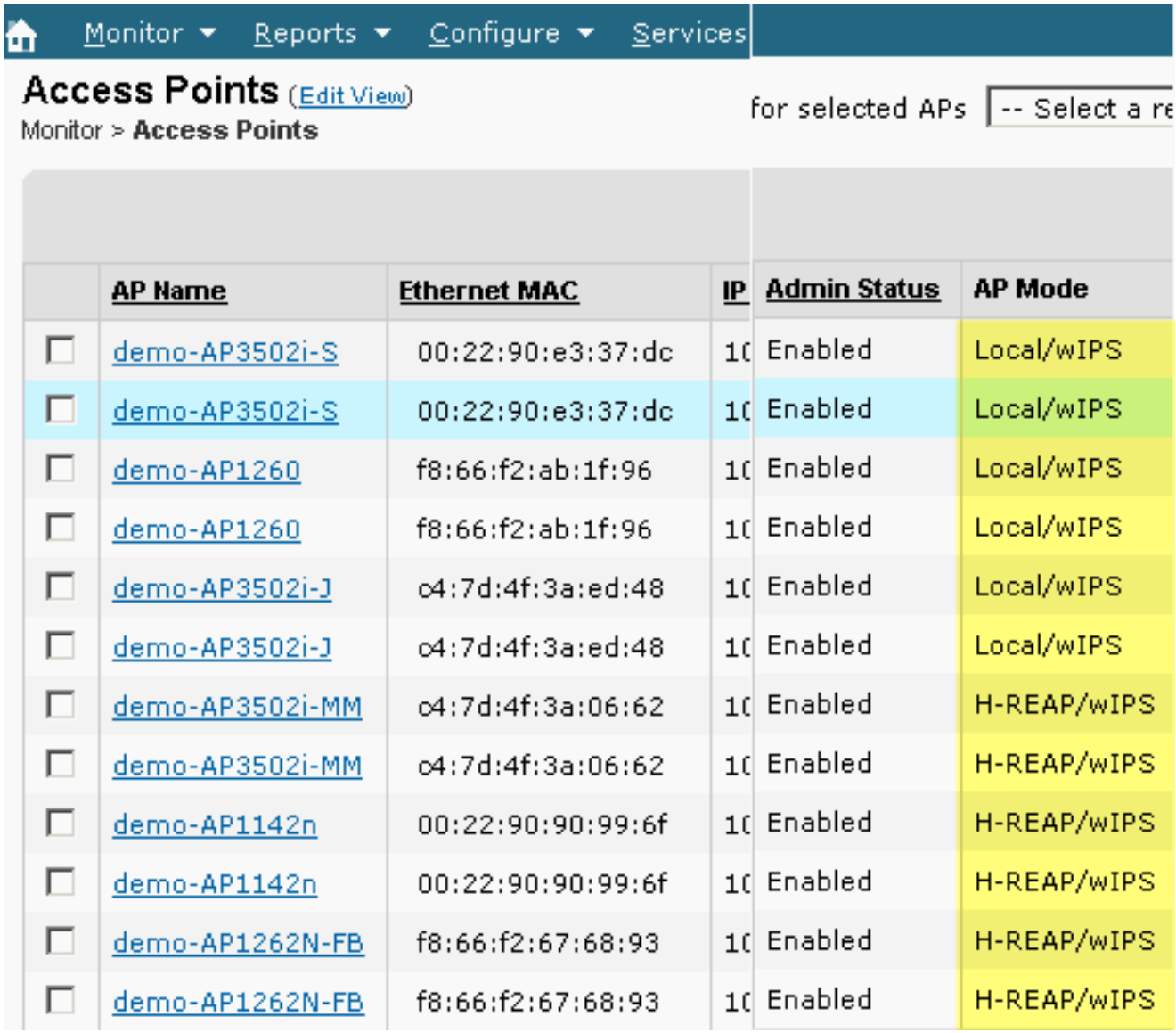
Remarque : si l'une des radios de ce point d'accès est activée, WCS ignorera la configuration et lancera l'erreur dans la Figure 7.

Figure 7 - Rappel WCS pour désactiver les points d'accès radio avant d'activer ELM



4. La réussite de la configuration peut être vérifiée en observant le changement dans le mode AP de « Local ou H-REAP » à Local/wIPS ou H-REAP/wIPS. Voir la figure 8.

Figure 8 - WCS affichant le mode AP pour inclure wIPS avec Local et/ou H-REAP

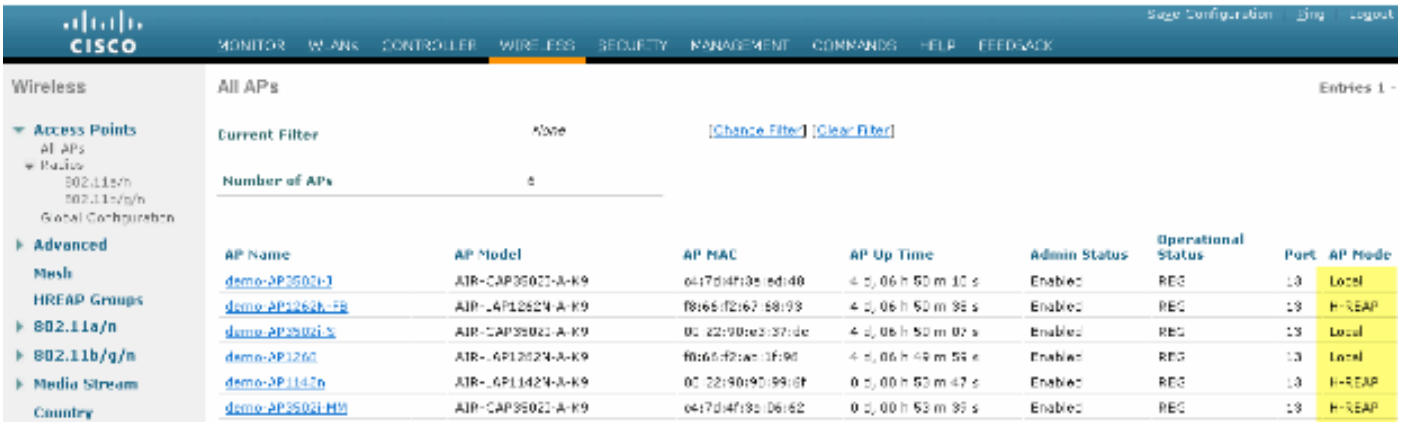


5. Activez les radios qui ont été désactivées à l'étape 1.
6. Créez le profil wIPS et envoyez-le au contrôleur afin que la configuration soit terminée.

   Remarque : pour obtenir des informations de configuration complètes sur wIPS, reportez-vous au Guide de déploiement de Cisco Adaptive wIPS.

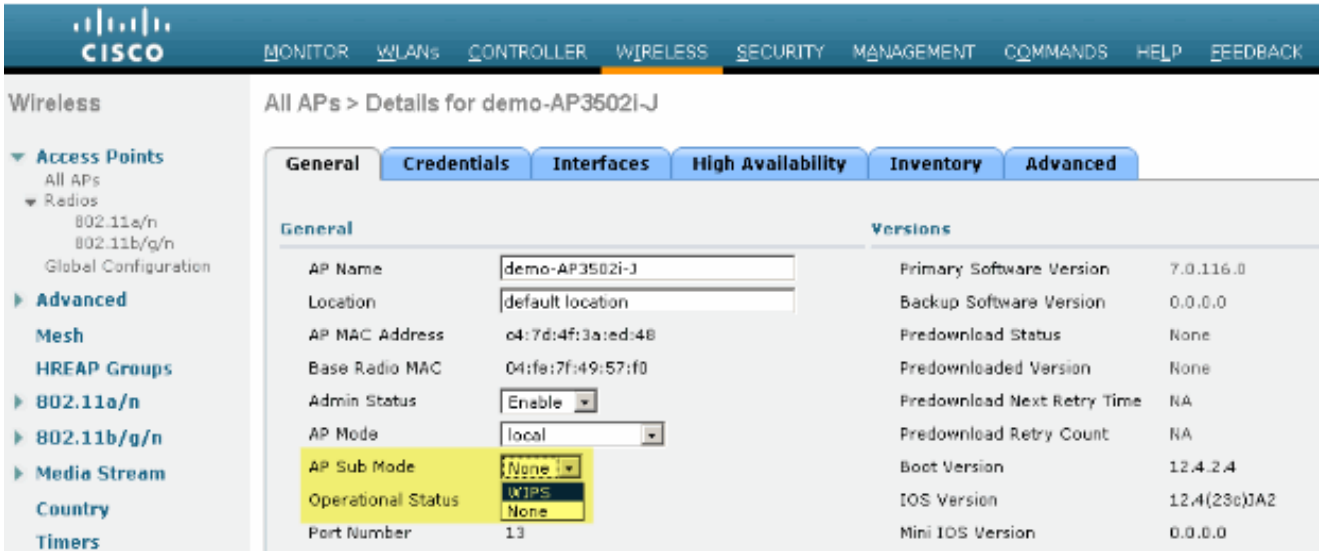
Configuration à partir du WLC

Figure 9 : configuration d'ELM avec WLC



1. Sélectionnez un point d'accès dans l'onglet Wireless.

   Figure 10 - WLC Changer le sous-mode AP pour inclure l'ELM wIPS



2. Dans le menu déroulant AP Sub Mode, choisissez wIPS (Figure 10).

3. Appliquez, puis enregistrez la configuration.

Remarque : pour que la fonctionnalité ELM fonctionne, MSE et WCS sont requis avec la licence wIPS. La modification du sous-mode AP du WLC seul n'activera pas ELM.

Attaques détectées dans ELM

Tableau 1 - Matrice de prise en charge des signatures wIPS

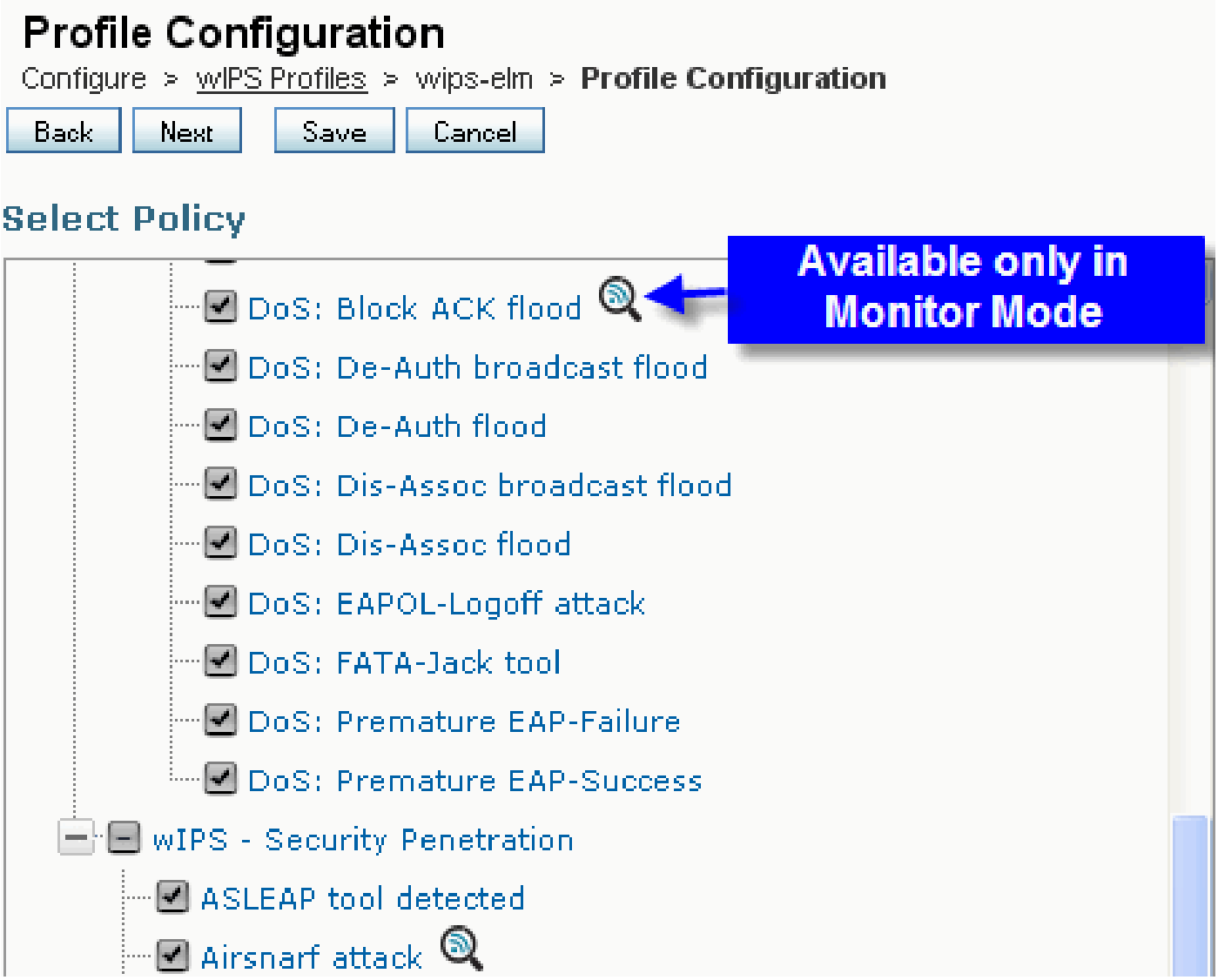
Attaques détectées	ORME	MM
Attaque DoS contre AP		
Inondation D'Association	O	O
Débordement de table d'association	O	O
Inondation D'Authentification	O	O
attaque EAPOL-Start	O	O

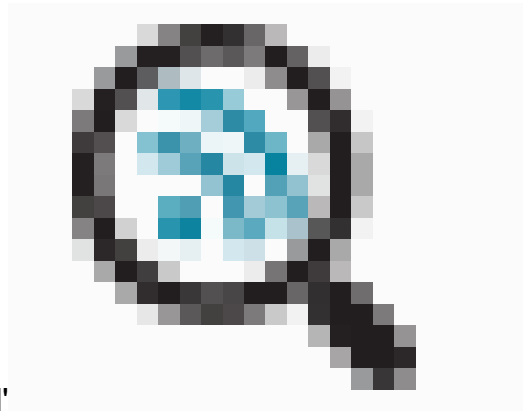
inondation due à PS-Poll	O	O
Inondation de demande de sonde	n	O
Association non authentifiée	O	O
Attaque DoS contre l'infrastructure		
crue de type CTS	n	O
Université de technologie du Queensland	n	O
brouillage RF	O	O
crue RTS	n	O
Attaque par opérateur virtuel	n	O
Attaque DoS contre une station		
Attaque d'échec d'authentification	O	O
Bloc ACK flood	n	O
Désauth broadcast flood	O	O
Délestage	O	O
Inondation de diffusion Dis-Assoc	O	O
crue de Dis-Assoc	O	O
attaque EAPOL-Logoff	O	O
outil FATA-Jack	O	O
EAP-Failure prématurée	O	O
EAP-Success prématuré	O	O
Attaques par pénétration de sécurité		
Outil ASLEAP détecté	O	O
attaque par Airsnarf	n	O
Attaque ChopChop	O	O
Attaque Day-Zero par anomalie de sécurité WLAN	n	O
Attaque Day-Zero par anomalie de sécurité des appareils	n	O
Sondage de périphériques pour AP	O	O
Attaque de dictionnaire sur les méthodes EAP	O	O
Attaque EAP contre authentification 802.1x	O	O
Faux points d'accès détectés	O	O
Faux serveur DHCP détecté	n	O

Outil de détection de fissure FAST WEP	O	O
Attaque par fragmentation	O	O
Point d'accès Honeypot détecté	O	O
Outil Hotspotter détecté	n	O
Trames de diffusion incorrectes	n	O
Paquets 802.11 mal formés détectés	O	O
Attaque de l'homme du milieu	O	O
Netstumbler détecté	O	O
Victime de Netstumbler détectée	O	O
Violation PSPF détectée	O	O
Point d'accès logiciel ou hôte détecté	O	O
Adresse MAC usurpée détectée	O	O
Trafic suspect en dehors des heures de bureau détecté	O	O
Association non autorisée par liste de fournisseurs	n	O
Association non autorisée détectée	O	O
Wellenreiter détecté	O	O

Remarque : l'ajout de CleanAir permet également de détecter les attaques non 802.11.

Figure 11 - Vue du profil WCS wIPS





Dans la Figure 11, configurez le profil wIPS à partir de WCS, l' icône indique que l'attaque sera détectée seulement quand AP est en MM, alors que seulement meilleur effort quand en ELM.

Dépannage d'ELM

Vérifiez les éléments suivants :

- Assurez-vous que NTP est configuré.

- Assurez-vous que l'heure MSE est définie en UTC.
- Si le groupe de périphériques ne fonctionne pas, utilisez le SSID de profil de superposition avec Any. Redémarrez l'AP.
- Assurez-vous que la licence est configurée (actuellement, les points d'accès ELM utilisent des licences KAM)
- Si les profils wIPS sont modifiés trop souvent, synchronisez à nouveau le contrôleur MSE. Assurez-vous que le profil est actif sur le WLC.
- Assurez-vous que WLC fait partie de MSE en utilisant les CLI MSE :

    1. SSH ou Telnet vers votre MSE.
    2. Execute /opt/mse/wips/bin/wips_cli - Cette console peut être utilisée pour accéder aux commandes suivantes afin de collecter des informations concernant l'état du système wIPS adaptatif.
    3. show wlc all - Problème dans la console wIPS. Cette commande est utilisée pour vérifier les contrôleurs qui communiquent activement avec le service wIPS sur le MSE. Voir la figure 12.

        Figure 12 - CLI MSE Vérification de l'activité du WLC avec les services MSE wIPS

        <#root>

        ```
        wIPS>

        show wlc all


        WLC MAC              Profile             Profile
        Status                  IP
        Onx Status Status
        ------------------------------------------------
        ------------------------------------------------
        ----
        00:21:55:06:F2:80    WCS-Default         Policy
        active on controller     172.20.226.197
        Active
        ```

- Assurez-vous que des alarmes sont détectées sur MSE à l'aide des CLI MSE.
    - show alarm list - Problème au sein de la console wIPS. Cette commande est utilisée pour répertorier les alarmes actuellement contenues dans la base de données du service wIPS. Le champ clé est la clé de hachage unique attribuée à l'alarme spécifique. Le champ Type indique le type d'alarme. Ce graphique de la Figure 13 présente une liste d'ID d'alarme et leurs descriptions :

        Figure 13 : commande show alarm list de l'interface de ligne de commande MSE

<#root>

wIPS>

show alarm list

```
Key         Type  Src MAC
LastTime              Active          First Time
-----------------------------------------------
-----------------------------------------
89          89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631       95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183     99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

Les champs First Time et Last Time indiquent les horodatages de détection de l'alarme ; ils sont stockés en heure UTC. Le champ Actif s'affiche en surbrillance si l'alarme est actuellement détectée.

- Effacez la base de données MSE.
  - Si vous vous trouvez dans une situation où la base de données MSE est corrompue, ou si aucune autre méthode de dépannage ne fonctionne, il peut être préférable d'effacer la base de données et de recommencer.

  Figure 14 : commande MSE services

```
1. /etc/init.d/msed stop
2. Remove the database using the command 'rm
/opt/mse/locserver/db/linux/server-eng.db'
3. /etc/init.d/msed start
```

Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0
- Guide de configuration de Cisco Wireless Control System, version 7.0.172.0
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.