Module de Cisco Aironet AP pour le guide de sécurité sans fil et de déploiement de l'intelligence de spectre (WSSI)

Contenu

Introduction

Ce document fournit des instructions de configuration générale et de déploiement pour le module de Point d'accès de Cisco Aironet pour l'intelligence de sécurité sans fil et de spectre (WSSI). Le WSSI est un module ajouté qui peut être inséré dans les Points d'accès modulaires (aps) comme la gamme Cisco 3600 AP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Le module d'intelligence de sécurité sans fil et de spectre a besoin des versions de code minimal :

- Contrôleur LAN Sans fil (WLC) – Version 7.4.xx.xx ou plus tard
- Point d'accès (AP) – Version 7.4.xx.xx ou plus tard
- Infrastructure principale (pi) – Version 1.3.xx.xx ou plus tard
- Engine de Services de mobilité (MSE) – Version 7.4.xx.xx ou plus tard

Conventions

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

Présentation du produit

Le module d'intelligence de sécurité Cisco Wireless et de spectre, tirant profit de la conception modulaire flexible de la gamme 3600 AP de Cisco Aironet, livre sans précédent, toujours-sur la lecture de Sécurité et l'intelligence de spectre. Ceci vous aide à éviter l'interférence de Radiofréquence (RF) de sorte que vous obteniez une meilleures couverture et représentation sur votre réseau Sans fil.

- Moniteur et réduction de large spectre de 24 heures sur 24, 7 jours sur 7 pour l'aWIPS, le CleanAir, la connaissance de contexte, la détection escroc et la gestion des ressources de radio
- Protection contre les menaces d'aWIPS de sur-canal de 24 heures sur 24, 7 jours sur 7
- 23 fois plus de couverture de Sécurité et de spectre
- Économies de coûts 30%+ CAPEX contre le mode moniteur dédié AP
- Configuration zéro de toucher

Le module champ-extensible WSSI est une radio dédiée qui débarque toute la surveillance et les Services de sécurité des radios de client/service de données à la Sécurité surveillent le module. Ceci tient compte non seulement d'une meilleure représentation de client, mais réduit également des coûts en éliminant le besoin de mode moniteur dédié aps et l'infrastructure Ethernet exigée pour connecter ces périphériques dans leur réseau.

Ensemble, la gamme 3600 aps et enable de module WSSI vous pour fournir simultanément la Sécurité et l'analyse du spectre de pointe fonctionne pour des clients de Wi-Fi sur tous les canaux, dans les bandes 2.4-GHz et 5-GHz.

Une fois que déployé, le module balaye constamment tous les canaux pour aider à assurer les la plupart sécurisées et une expérience Sans fil robuste disponible dans le secteur.

Avantages de mode WSSI

Mode local amélioré (ORME) :

- Réduit des coûts du réseau et des exécutions. En intégrant le module WSSI dans la gamme 3600, vous pouvez remplacer jusqu'à trois périphériques distincts. Ceci fournit trois fonctions

distinctes dans une seule, universelle gamme 3600 AP.
- Les clients peuvent maintenant accroître une connexion Ethernet simple (câble et port) dans leur réseau câblé, au lieu de ce qui exigerait typiquement jusqu'à trois câbles Ethernet distincts et un port d'accès dans leur réseau câblé. Ceci réduit de manière significative leur CAPEX.
- En intégrant toutes ces caractéristiques à AP simple, les clients simplifient la Gestion et la surveillance de jour en jour de leur infrastructure et réseau Sans fil avec un nombre d'aps considérablement réduit. Le module WSSI apparaît au WLC et aux systèmes de gestion comme radio supplémentaire prenant en charge les périphériques du client 802.11b/g/a/n (2.4 et 5 gigahertz) dans la gamme 3600 spécifique AP.
- *La configuration zéro de toucher*, installent, mise sous tension et disparaissent. Il n'y a absolument aucune configuration exigée pour permettre au module WSSI d'être en service, et immédiatement surveillant et sécurisant votre réseau Sans fil. Le module WSSI est inséré et sécurisé à n'importe quelle gamme 3600 AP. Quand AP est actionné sauvegardez le module est initialisé avec les autres radios dans AP et commence immédiatement surveillant tous les canaux sur 2.4 et 5 gigahertz pour toutes les menaces de sécurité potentielle et sources d'interférence.
- Le wIPS adaptatif fournit la détection précise et efficace de menace sur tous les canaux de au-dessus - des attaques aériennes, les aps escrocs, et les connexions ad hoc, aussi bien que la capacité de classifier, annoncer, atténuer et signaler pour la surveillance et l'administration proactive constantes. Les travaux en même temps que la mobilité Cisco entretient l'engine (MSE).

ORME :

- Ajoute la lecture de Sécurité de wIPS pour 7x24 sur la lecture de canal (2.4GHz et 5 gigahertz), avec le meilleur effort outre du support de canal.
- AP sert supplémentaire des clients et avec la gamme G2 d'aps, analyse du spectre de CleanAir d'enables sur des canaux (2.4GHz et 5GHz).

Mode moniteur :

- Le mode moniteur AP (MMAP) est dédié pour fonctionner dans le mode moniteur et a l'option d'ajouter la lecture de Sécurité de wIPS de tous les canaux (2.4GHz et 5GHz).
- La gamme G2 d'aps active l'analyse du spectre de CleanAir sur tous les canaux (2.4GHz et 5GHz).
- MMAPs ne servent pas des clients.

AP3600 avec le module WSSI : L'évolution de la sécurité sans fil et du spectre

- Premier AP du secteur qui facilite le service clientèle, la lecture de Sécurité de wIPS et l'analyse du spectre simultanés utilisant la technologie de CleanAir.
- 2.4GHz et 5GHz dédiés transmettent par radio avec ses propres Antennes qui activent la lecture 7x24 de tous les canaux Sans fil dans les bandes 2.4GHz et 5GHz.
- Une infrastructure Ethernet simple fournit à l'exécution simplifiée moins périphériques pour gérer et retour sur l'investissement optimisé de l'infrastructure AP3600 Sans fil et de l'infrastructure câblée d'Ethernets.

- Technologie de Cisco CleanAir : fournit l'intelligence proactive et ultra-rapide de spectre de combattre des problèmes de performances dus à l'interférence Sans fil. La première technologie de pointe d'analyse rf du secteur qui examine et classifie les modèles d'énergie

(signatures) des périphériques qui peuvent de manière significative affecter la qualité d'un réseau Sans fil.
- Gestion des ressources radio (RRM) : la Gestion simplifiée et avancée rf, s'adapte automatiquement à l'environnement de réseau Sans fil basé sur les informations reçues de la technologie de Cisco CleanAir. Une fois que des interferers sont identifiés, RRM peut déplacer des périphériques de client aux canaux à partir de l'interférence et ajuster l'alimentation de transit de s'éloigner de la source d'interférence. Ceci fournit une meilleure qualité rf à l'utilisateur.
- Détection escroc : détecte et signale l'accès au réseau et l'accès secrets aux clients sans fil.
- Connaissance d'emplacement et de contexte : fournit la connaissance en temps réel et la capacité de dépister le point final Sans fil.

Avec ces configurations, le module d'intelligence de sécurité Cisco Wireless et de spectre, avec la gamme Cisco 3600 AP, fournit le réseau Sans fil de classe entreprise sécurisée et robuste de la plupart possible pour vos utilisateurs en entreprise et données.

Sur-canal contre le Hors fonction-canal utilisant le module WSSI

Un mode local AP balaye pour le sur-canal d'attaquants d'interferers et de wIPs de CleanAir. Ceci signifie les balayages AP seulement le canal qu'il sert. Un mode local AP avec un canal de service de la radio 2.4GHz 1 et le canal de service 5GHz par radio 64, assure seulement la protection sur les canaux 1 et 64.

Un MMAP balaye pour le hors fonction-canal d'attaquants d'interferers et de wIPs de CleanAir. Ceci signifie qu'AP balaye tous les canaux. La radio 2.4GHz balaye tous les canaux 2.4GHz et le canal 5GHz balaye tous les canaux 5GHz.

Une gamme Cisco 3600 AP utilise une combinaison de sur-canal et de hors fonction-canal. Les radios 2.4GHz et 5GHz balayent le sur-canal et le module WSSI balaye le hors fonction-canal, faisant un cycle entre tous les canaux 2.4GHz et 5GHz.

Densité suggérée de déploiement pour le module WSSI

Dans le déploiement traditionnel du moniteur AP, Cisco recommande un rapport de 1 MMAP à chaque 5 mode local aps. Ceci peut varier basé sur la conception de réseaux et les conseils d'expert pour la meilleure couverture. Avec le module WSSI, il y a différentes recommandations de déploiement basées sur la fonctionnalité pour réaliser la parité de couverture avec un MMAP.

Pour CleanAir, il est recommandé pour déployer 1 module WSSI pour chaque 5 locaux ou Flexconnect aps. Ce déploiement de 1:5 offre la même représentation qu'un MMAP activé par CleanAir, mais permet toujours à AP pour servir des clients. C'est un déploiement recommandé pour un module WSSI exécutant CleanAir :

Pour la protection de wIPS, il est recommandé pour déployer 2 modules WSSI pour chaque 5 locaux ou FlexConnect aps. La période de détection de wIPS pour une attaque de hors fonction-canal est environ deux fois qui d'un MMAP. Par conséquent, un déploiement de 2:5 est exigé pour fournir la parité de détection de wIPS. C'est le déploiement recommandé pour un module WSSI exécutant la protection de wIPS :

Le Cisco 3600 AP avec un module WSSI utilise le sur-canal et la lecture de hors fonction-canal pour fournir une solution de pointe tout en servant des clients.

Installer le module WSSI

Configuration pour le module AP3600 WSSI

Il n'y a aucune configuration pour le module WSSI requis. Le module balaye automatiquement tous les canaux sur les deux bandes utilisant son 0x4 les Antennes (uniquement réceptrices) de 0 Tx X 4 Antennes de Rx.

Notez que le module WSSI est seulement en activité sur AP3600s configuré en mode local ou mode de FlexConnect. Le module WSSI est désactivé en tous autres modes.

Puissance requise pour le module WSSI

L'AP3600 avec un module WSSI installé dépasse 15.4 watts (802.3af). AP exige l'un ou l'autre (802.3at - PoE+), PoE amélioré, un approvisionnement local d'alimentation AC, ou l'injecteur de Cisco PoE (AIR-PWRINJ4).

Remarques :

- Le PoE amélioré a été créé par Cisco et est un précurseur à 802.3at PoE+. Il fournit jusqu'à 20W de l'alimentation.
- PoE+ peut livrer jusqu'à 30W de l'alimentation.

Gestion des ressources par radio sur le module WSSI

Le module WSSI prend toutes les mesures RRM sur la bande la bande 2.4GHz et le 5GHz. Les mesures sont affichées dans le GUI WLC sous le moniteur > les Points d'accès > le 802.11a/n > l'AP_NAME > les détails ou le moniteur > les Points d'accès > le 802.11b/g/n > l'AP_NAME > les détails.

CleanAir sur le module WSSI

Le module WSSI détecte des interferers de CleanAir avec la même précision qu'un MMAP. Cisco recommande que le module WSSI soit déployé avec une densité de 1:5, où il doit y avoir 1 module WSSI pour chaque 5 aps. C'est la même densité recommandée que pour un MMAP.

Quand le module WSSI est activé sans le sous-modèle, le module balaye la bande la bande 2.4GHz et le 5GHz. Le module insiste sur chaque canal pour 1.2secs et balaye pour des interferers de CleanAir.

CleanAir peut être activé sur 2.4GHz seulement, 5GHz seulement, et 2.4GHz et 5GHz. C'est sélectionable du WLC CLI ou du GUI. Voici un exemple de configurer CleanAir sur le WLC CLI :

```
(Cisco Controller) >config 802.11-abgn cleanair enable APNAME 2.4GHz
(Cisco Controller) >config 802.11-abgn cleanair enable APNAME 5GHz
```

La même configuration peut être appliquée sur le GUI par l'intermédiaire de la radio > les radios à deux bandes > configurent. Voici un exemple de ceci :

Afin de vérifier que l'interferer de CleanAir a été détecté par le module WSSI, émettez les **interferers de cleanair d'exposition** commandent de la console AP :

```
SJC14-21A-AP-DUNGENESS-X# show cleanair interferers
CleanAir: slot 0 band 2.4 number of devices 0:
CleanAir: slot 1 band 5.0 number of devices 0:
CleanAir: slot 2 band 2.4 number of devices 0:
CleanAir: slot 2 band 5.0 number of devices 1:
IDR: 24(3159) Video Camera
     ISI=0, -74 dBm, duty=100
     c=00180000 sig(4)=1057CA80
     on/report/seen 22/22/22 secs ago
```

La même configuration peut être appliquée sur le GUI par l'intermédiaire de la radio > les radios à deux bandes > configurent. Voici un exemple :

Les interferers de CleanAir sont signalés au GUI WLC. Interferers sont affichés PAR BANDE. Ceci signifie que des interferers détectés sur le module WSSI sur la bande 5GHz sont affichés sous le moniteur > le 802.11a/n > les périphériques d'interférence.

Afin de vérifier que l'interferer de CleanAir a été détecté par le module WSSI, émettez les **interferers de cleanair d'exposition de la** console AP :

```
SJC14-21A-AP-DUNGENESS-X# show cleanair interferers
CleanAir: slot 0 band 2.4 number of devices 0:
CleanAir: slot 1 band 5.0 number of devices 0:
CleanAir: slot 2 band 2.4 number of devices 0:
CleanAir: slot 2 band 5.0 number of devices 1:
IDR: 24(3159) Video Camera
     ISI=0, -74 dBm, duty=100
     c=00180000 sig(4)=1057CA80
     on/report/seen 22/22/22 secs ago
```

wIPS sur le module WSSI

Le module WSSI détecte des attaquants de wIPS avec presque la même précision qu'un MMAP. Pour le wIPS, Cisco recommande déployer le module WSSI avec un rapport de 2:5 parmi des aps. Ce les moyens pour chaque 5 aps, deux des aps doivent contenir le module WSSI.

Il y a deux modes de wIPS qui peuvent être configurés :

- sous-mode de wIPS - La détection d'attaque de wIPS d'enables et balaye tous les canaux pour 1.2s. Ce mode permet à AP pour capturer toujours tous les états RRM en plus des détections de wIPS.
- Mode amélioré de wIPS - Activez la détection d'attaque de wIPS et balayez tous les canaux pour 250ms. Le temps de pause plus petit de canal permet au module de Sécurité pour détecter des attaquants plus vite.

De la page principale de l'infrastructure (pi), allez configurer > Acesss se dirige > AP_NAME. Le module WSSI peut être configuré au sous-mode de wIPS ou au sous-mode de wIPS + support de moteur amélioré de wIPS. Ceci peut également être poussé en tant qu'élément d'un modèle de configuration AP.

Les attaques de wIPS sont affichées à l'infrastructure principale de la maison > de l'onglet Sécurité.

Pi affiche une vue de niveau du réseau, mais vous pouvez afficher l'attaque sur un AP3600 avec un module WSSI en émettant la commande de l'**alarme ALARM_NUM du capwap AM d'exposition de la** console AP.

Par exemple, l'alarme 52 est un Déni de service, inondation d'authentification. Afin de voir si cette attaque était détectée sur le module WSSI, émettez la commande de l'**alarme 52 du capwap AM d'exposition** :

```
SJC14-21A-AP-DUNGENESS-X# show capw am alarm 52
capwap_am_show_alarm = 52

<A id='47C30C9E'>
<AT>52</AT>
<FT>2012/10/01 21:04:22</FT>
<LT>2012/10/01 21:04:49</LT>
<DT>2012/10/01 18:49:08</DT>
<SM>00:40:96:B5:85:8D-a</SM> <SNT>2</SNT>
<DM>00:22:55:F2:80:9F-a</DM> <DNT>1</DNT>
 <CH>11</CH>
 <FID>0</FID>
 pAlarm.bPendingUpload = 0
```

L'escroc les détectent sur le module WSSI

Le module WSSI détecte des aps escrocs avec la même précision qu'un MMAP. Une liste de l'escroc aps est affichée dans le WLC et pi.

C'est la liste de l'escroc non classifié aps du GUI WLC. Des aps escrocs peuvent être visualisés dans le GUI WLC sous le moniteur > les escrocs.

Vous pouvez vérifier que le module WSSI utilisant la console AP a détecté un escroc AP. De la console, présentez l'**escroc AP d2 de rm de capwap d'exposition toute la** commande. Ceci affiche tout l'escroc aps vu à la radio de module WSSI.

```
SJC14-21A-AP-DUNGENESS-X# show capwap rm rogue ap dot11radio2 all
 ****************** CURRENT ROGUE APS ****************

ROGUE AP: 0  BSSID = 64:D9:89:42:24:3E, channel = 149
SSID = alpha_phone
heard 7 seconds ago
authFailedCount=0
NumOfPkts = 2, wep = 1, SP = 0, adHoc = 0, wpa = 1, 11g = 0, 11n=2
antenna 1 pkts 2 avgRssi -81 avgSnr 13


 ****************** MASTER ROGUE APS ****************

ROGUE AP: 0  BSSID = C4:3D:C7:8A:EE:90, channel = 1
SSID = NETGEAR_11ng
heard 7 seconds ago
authFailedCount=0
isBeingContained = 0
seen at 0 seconds for 0 times and valid = 1
NumOfPkts = 16108, wep = 0, SP = 1, adHoc = 0, wpa = 0, 11g = 1, 11n=2
antenna 1 pkts 16108 avgRssi -73 avgSnr 12

ROGUE AP: 1  BSSID = EC:44:76:81:C0:02, channel = 1
SSID = alpha_byod
heard 151 seconds ago
authFailedCount=0
isBeingContained = 0
seen at 0 seconds for 0 times and valid = 1
NumOfPkts = 413, wep = 1, SP = 1, adHoc = 0, wpa = 1, 11g = 1, 11n=2
```

```
antenna 1 pkts 413 avgRssi -84 avgSnr 5
```

Retenue escroc utilisant le module WSSI

Le module WSSI est un module 0x4 (recevez les Antennes seulement), signifiant que la retenue d'escroc sera exécutée sur la radio 2.4GHz ou 5GHz. Afin de configurer le WSSI pour contenir automatiquement des aps escrocs, vous devez s'assurer que dans le GUI WLC dans le cadre des stratégies de Sécurité > de protection sans fil > débarrassez des plants peu vigoureux les stratégies > le général que la **retenue automatique seulement pour le mode moniteur aps** n'est pas activée (voyez le tir d'écran suivant). Toutes autres cases peuvent être activées.

Averti-emplacement de contexte sur le module WSSI

Une fois lié à Cisco MSE, le module WSSI fournit le cadre averti – des données d'emplacement avec la même précision qu'un MMAP.

Autorisation de module WSSI

Le module WSSI utilise des permis de mode moniteur de wIPS.

Informations connexes

- Support et documentation techniques - Cisco Systems