Le wIPS adaptatif de Cisco a amélioré la configuration de mode local (ORME) et le guide de déploiement

Contenu

Introduction

La solution Sans fil adaptative de système de prévention des intrusions de Cisco (wIPS) ajoute la caractéristique améliorée de mode local (ORME), permettant à des administrateurs pour utiliser leurs Points d'accès déployés (aps) pour assurer la protection complète sans besoin de réseau de substitution distinct (le schéma 1). Avant l'ORME et dans le déploiement adaptatif traditionnel de wIPS, le mode moniteur dédié (millimètre) aps sont exigés pour assurer les besoins ou la protection de conformité PCI contre l'accès sécurisé, la traversée, et les attaques non autorisés (le schéma 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 seulement sur l'ORME et ne modifie aucun avantage existant de déploiement de wIPS avec le millimètre aps.

Figure 1 - Déploiement amélioré du mode local AP Figure 2 - Menaces supérieures de sécurité sans fil

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Éléments requis d'ORME et versions de code minimal

- Contrôleur LAN Sans fil (WLC) - Version 7.0.116.xx ou ultérieures
- Aps - Version 7.0.116.xx ou ultérieures
- Système de contrôle sans fil (WCS) - Version 7.0.172.xx ou ultérieures
- Engine de Services de mobilité - Version 7.0.201.xx ou ultérieures

Prendre en charge des Plateformes WLC

L'ORME est pris en charge sur des Plateformes WLC5508, WLC4400, WLC 2106,WLC2504, WiSM-1, et WiSM-2WLC.

Prendre en charge des aps

L'ORME est pris en charge sur 11n aps comprenant 3500, 1250, 1260, 1040, et 1140.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Écoulement d'alarme de wIPS d'ORME

Les attaques sont seulement appropriées quand elles se produisent sur l'infrastructure de confiance aps. L'ORME aps le détectera et communiquera au contrôleur et à la corrélation avec le MSE pour signaler avec la Gestion WCS. La figure 3 fournit l'écoulement d'alarme du point de vue d'un administrateur :

1. Attaque lancée contre un périphérique d'infrastructure (« de confiance » AP)
2. Détecté sur l'ORME AP a communiqué par CAPWAP à WLC
3. Passé d'une manière transparente à MSE par l'intermédiaire de NMSP
4. Connecté dans la base de données de wIPS sur MSE envoyé à WCS par l'intermédiaire du déroutement SNMP
5. Affiché à WCS

Figure 3 - Détection de menace et écoulement d'alarme

Considérations de déploiement pour l'ORME

Cisco recommande cela en activant l'ORME sur chaque AP sur le rassemblement de réseau la plupart des besoins de Sécurité de client quand un recouvrement et/ou les coûts de réseau font partie de considération. La caractéristique primaire d'ORME fonctionne efficacement pour des attaques de sur-canal, sans n'importe quelle compromission à la représentation sur des données, des clients de Voix et de vidéo, et des services.

ORME contre le millimètre dédié

La figure 4 fournit un contraste général entre les déploiements standard du wIPS le millimètre aps et l'ORME. Dans l'examen, la plage de couverture typique pour les deux modes suggère :

- Le wIPS dédié le millimètre AP couvre typiquement 15,000-35,000 pieds carrés
- le Client-service AP couvrira typiquement de 3,000-5,000 pieds carrés

Figure 4 - Recouvrement de millimètre contre tout l'ORME aps

Dans le déploiement adaptatif traditionnel de wIPS, Cisco recommande un rapport de 1 millimètre AP à chaque 5 mode local aps, qui peut également varier basé sur la conception de réseaux et les conseils d'expert pour la meilleure couverture. En considérant l'ORME, l'administrateur active simplement la caractéristique de logiciel d'ORME pour tous les aps existants, ajoutant efficacement des exécutions de wIPS millimètre au mode local AP de donnée-service tout en mettant à jour la représentation.

Sur-canal et représentation de Hors fonction-canal

UN millimètre AP utilise 100% du moment de la radio pour balayer tous les canaux, car il ne sert aucun client WLAN. La caractéristique primaire pour l'ORME fonctionne efficacement pour des attaques de sur-canal, sans n'importe quelle compromission à la représentation sur des données, Voix et des clients et des services de vidéo. La différence principale est dans la lecture variable de hors fonction-canal de mode local ; selon l'activité, la lecture de hors fonction-canal fournit le temps de pause minimal de recueillir assez d'informations disponibles pour classifier et déterminer l'attaque. Un exemple peut être avec les clients de Voix qui sont associés et où la lecture RRM d'AP est reportée jusqu'à ce que le client de Voix soit dissocié pour s'assurer service n'est pas affectée. Pour cette considération, la détection d'ORME pendant le hors fonction-canal est considérée meilleur effort. ORME voisin aps fonctionnant sur tous, pays ou efficacité d'augmentations de canaux DCA, par conséquent la recommandation pour activer l'ORME sur chaque mode local AP pour la couverture de protection maximale. Si la condition requise est pour la lecture dédiée sur tous les canaux à plein temps, la recommandation sera de déployer le millimètre aps.

Ces points passent en revue des différences du mode local et du millimètre aps :

- Mode local AP - Les clients WLAN de services avec la lecture de hors fonction-canal de découpage de temps, écoute 50ms sur chaque canal, et lecture configurable de caractéristiques pour des canaux de tous/country/DCA.
- Mode moniteur AP - Ne sert pas des clients WLAN, dédiés au balayage seulement, écoute 1.2s sur chaque canal, et balaye tous les canaux.

ORME à travers des liens WAN

Cisco a fait de grands efforts afin d'optimiser des caractéristiques dans les scénarios provocants, tels que déployer l'ORME aps à travers des liens WAN de faible bande passante. La caractéristique d'ORME implique de prétraiter en déterminant des signatures d'attaque à AP et est optimisée pour fonctionner au-dessus des liens lents. Comme pratiques recommandées, il est recommandé pour tester et mesurer la spécification de base pour valider la représentation avec l'ORME au-dessus du WAN.

Intégration de CleanAir

La caractéristique d'ORME complimente fortement des exécutions de CleanAir avec la représentation semblable et des avantages au déploiement du millimètre aps avec ces avantages spectre-avertis existants de CleanAir :

- Intelligence niveau du silicium dédiée rf
- Spectre-averti, autocuratif, et auto-optimiser
- Menace de canal et détection et réduction d'interférence non standard
- Non détection de WiFi telle que Bluetooth, la micro-onde, les téléphones sans fil, etc.
- Détectez et localisez les attaques DoS de couche rf telles que des brouilleurs rf

Fonctionnalités et bénéfices d'ORME

- Lecture adaptative de wIPS dans les gens du pays et le H-REAP aps de service de données
- Protection sans exiger un réseau de substitution distinct
- Disponible comme téléchargement libre de SW pour les clients existants de wIPS
- Conformité PCI de supports pour les réseaux locaux Sans fil
- Pleins 802.11 et détection de l'attaque non-802.11
- Ajoute des médecines légales et des fonctions de création de rapports
- Intègre avec la Gestion existante CUWM et WLAN
- Flexibilité de placer le millimètre intégré ou dédié aps
- Le prétraitement aux aps réduisent la liaison de données (c'est-à-dire, fonctionne au-dessus très des liaisons à faible bande passante)
- Basse incidence sur les données de service

Autorisation d'ORME

Le wIPS d'ORME ajoute un nouveau permis à la commande :

- AIR-LM-WIPS-Xx - Permis de wIPS d'ORME de Cisco
- AIR-WIPS-AP-xx - Permis Sans fil de wIPS de Cisco

Notes supplémentaires en autorisation d'ORME :

- Si le permis UGS millimètre AP de wIPS sont déjà installés, ces permis peuvent également être utilisés pour l'ORME aps.
- les permis de wIPS et les permis d'ORME comptent ensemble vers les limites de permis de plate-forme pour l'engine de wIPS ; 2000 aps sur 3310, et 3000 aps sur 335x, respectivement.
- Le permis d'évaluation inclura 10 aps pour le wIPS et 10 pour l'ORME pendant une période de jusqu'à 60 jours. Avant l'ORME, le permis d'évaluation a permis jusqu'à 20 le wIPS le

millimètre aps. L'exigence minimum des versions de logiciel prenant en charge l'ORME doit être répondue.

Configurez l'ORME avec WCS

Figure 5 - Utilisant WCS pour configurer l'ORME

1. De WCS, désactivez les radios 802.11b/g et 802.11a d'AP avant l'activation « a amélioré l'engine de wIPS. »**Note**: Tous les clients associés seront déconnectés, et ne se joindront pas jusqu'à ce que les radios soient activées.
2. Configurez un AP, ou utilisez un modèle de configuration WCS pour le plusieurs poids léger aps. Voir la figure 6.**Figure 6 - Activez le mode amélioré de sous-titre d'engine de wIPS (ORME)**
3. Choisissez l'**engine améliorée de wIPS**, et cliquez sur la **sauvegarde**.L'activation de l'engine améliorée de wIPS ne fera pas redémarrer AP.H-REAP est pris en charge ; activez la même manière que pour le mode local AP.**Note**: Si l'un ou l'autre des radios de cet AP est activée, WCS ignorera la configuration et jettera l'erreur dans la figure 7.**Figure 7 - Rappel WCS pour désactiver des radios AP avant d'activer l'ORME**
4. Le succès de configuration peut être vérifié en observant le changement du mode AP des « gens du pays ou de H-REAP » aux **gens du pays/au wIPS** ou au **H-REAP/wIPS**. Voir la figure 8.**Figure 8 - WCS affichant le mode AP pour inclure le wIPS avec des gens du pays et/ou H-REAP**
5. Activez les radios qui là où désactivé dans l'étape 1.
6. Créez le profil de wIPS et poussez-le au contrôleur pour que la configuration se termine.**Note**: Pour les informations de configuration complètes sur le wIPS, référez-vous au guide adaptatif de déploiement de wIPS de Cisco.

Configuration de WLC

Figure 9 - Configurez l'ORME avec WLC

1. Choisissez AP de l'**onglet sans fil**.**Figure 10 - WLC changeant le sous mode AP pour inclure l'ORME de wIPS**
2. Du menu déroulant de mode de sous-titre AP, choisissez le **wIPS** (le schéma 10).
3. Appliquez, et puis sauvegardez la configuration.

Note: Pour que la fonctionnalité d'ORME fonctionne, MSE et WCS sont exigés avec l'autorisation de wIPS. Changer le mode de sous-titre AP seul de WLC n'activera pas l'ORME.

Attaques détectées dans l'ORME

Tableau 1 - tableau de prise en charge de signatures de wIPS

Attaques détectées	ORME	Millimètre
Attaque DoS contre AP		
Inondation d'association	Y	Y
Dépassement de table d'associations	Y	Y
Inondation d'authentification	Y	Y

Attaque d'EAPOL-commencement	Y	Y
Inondation de Picoseconde-balayage	Y	Y
Inondation de demande de sonde	N	Y
Association Unauthenticated	Y	Y
Attaque DoS contre l'infrastructure		
Inondation CTS	N	Y
Université de technologie du Queensland l'exploit	N	Y
Bloquer rf	Y	Y
Inondation de RTS	N	Y
Attaque virtuelle de transporteur	N	Y
Attaque DoS contre la station		
Attaque d'échec d'authentification	Y	Y
Inondation du bloc ACK	N	Y
Inondation de l'émission De-Auth	Y	Y
Inondation De-Auth	Y	Y
Inondation d'émission de dis-Assoc	Y	Y
Inondation de dis-Assoc	Y	Y
Attaque d'EAPOL-déconnexion	Y	Y
Outil de FATA-connecteur	Y	Y
Eap-panne prématurée	Y	Y
Eap-succès prématuré	Y	Y
Attaques de traversée de Sécurité		
Outil ASLEAP détecté	Y	Y
Attaque d'Airsnarf	N	Y
Attaque de ChopChop	Y	Y
Attaque de jour-Zéro par anomalie de Sécurité WLAN	N	Y
Attaque de jour-Zéro par anomalie de sécurité des périphériques	N	Y
Périphérique sondant pour des aps	Y	Y
Attaque par dictionnaire sur des méthodes d'EAP	Y	Y
Attaque d'EAP contre l'authentification de 802.1x	Y	Y
Faux aps détecté	Y	Y
Faux serveur DHCP détecté	N	Y
Outil RAPIDE de fente WEP détecté	Y	Y
Attaque de fragmentation	Y	Y
Pot à miel AP détecté	Y	Y
Outil de Hotspotter détecté	N	Y
Trames inexactes d'émission	N	Y

Paquets mal formés de 802.11 détectés	Y	Y
Homme dans l'attaque moyenne	Y	Y
Netstumbler l'a détecté	Y	Y
Victime de Netstumbler détectée	Y	Y
Violation PSPF détectée	Y	Y
AP doux ou hôte AP détecté	Y	Y
Adresse MAC charriée détectée	Y	Y
Méfiant après le trafic d'heures détecté	Y	Y
Association non autorisée par la liste de constructeur	N	Y
Association non autorisée détectée	Y	Y
Wellenreiter l'a détecté	Y	Y

Note: Ajouter CleanAir activera également la détection des attaques non-802.11.

Figure 11 - Vue de profil de wIPS WCS

Dans la figure 11, configurez le profil de wIPS de WCS, le graphisme indique que l'attaque sera détectée seulement quand AP est dans le millimètre, tandis que seulement meilleur effort quand dans l'ORME.

Dépannez l'ORME

Vérifiez ces éléments :

- Assurez-vous que le NTP est configuré.
- Assurez-vous que paramètre horaire MSE est dans l'UTC.
- Si le groupe de périphériques ne fonctionne pas, en utilisez le profil SSID de recouvrement avec. Redémarrez AP.
- L'autorisation Make sure est configurée (actuellement l'ORME aps utilisent des permis KAM)
- Si des profils de wIPS sont changés trop souvent, synchronisez le MSE-contrôleur de nouveau. Assurez-vous que le profil est en activité sur WLC.
- Assurez-vous que WLC fait partie de MSE utilisant MSE CLIs :SSH ou telnet à votre MSE.Exécutez **/opt/mse/wips/bin/wips_cli** - Cette console peut être utilisée pour accéder à aux commandes suivantes de recueillir des informations concernant l'état du système adaptatif de wIPS.**affichez la** question de **wlc entièrement** à l'intérieur de la console de wIPS. Cette commande est utilisée de vérifier les contrôleurs qui communiquent activement avec le service de wIPS sur le MSE. Voir la figure 12.**Figure 12 - MSE CLI vérifiant l'Active WLC avec des services de wIPS MSE**

```
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 les alarmes obtiennent les ont détecté sur MSE utilisant MSE CLIs.**affichez la liste d'alarme** - Émettez à l'intérieur de la console de wIPS. Cette commande est utilisée de répertorier les alarmes actuellement contenues dans la base de données de service de wIPS. La zone de tri est la seule clé d'informations parasites assignée à l'alarme spécifique. Le champ de type est le type d'alarme. Ce tableau dans la figure 13 affiche une liste d'id et de descriptions d'alarme :**Figure 13 - Commande de liste d'alarme d'exposition MSE CLI**

```
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 la première fois qu'et de la fois passée signifient les horodateurs où l'alarme a été détectée ; ceux-ci sont enregistrés dans le temps UTC. Le champ actif met en valeur si l'alarme est actuellement détectée.
- Effacez la base de données MSE.Si vous vous exécutez dans une situation où la base de données MSE est corrompue, ou aucun d'autres méthodes de dépannage fonctionnerez, il peut être le meilleur d'effacer la base de données et de recommencer.**Figure 14 - MSE entretient la commande**

```
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
```

Informations connexes

- Guide de configuration Sans fil de contrôleur LAN de Cisco, release 7.0.116.0
- Guide de configuration de Système de contrôle sans fil Cisco, release 7.0.172.0
- Support et documentation techniques - Cisco Systems