Exemple de configuration de la protection des trames de gestion (MFP) d'infrastructure avec WLC et LAP

Contenu

Introduction

Ce document présente une nouvelle fonctionnalité de sécurité dans le sans fil appelé Management Frame Protection (MFP). Ce document décrit également comment configurer MFP dans des périphériques d'infrastructure, tels que des points d'accès léger (LAP) et des contrôleurs de réseau local sans fil (WLC).

Conditions préalables

Conditions requises

- Connaissance de la configuration du WLC et du LAP pour le fonctionnement de base

- Connaissance de base des trames de gestion IEEE 802.11

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC de la gamme Cisco 2000 qui exécute le microprogramme version 4.1
- LAP Cisco 1131AG
- Adaptateur client Cisco Aironet 802.11a/b/g qui exécute le microprogramme version 3.6
- Utilitaire Cisco Aironet Desktop Version 3.6

Remarque : MFP est pris en charge à partir des versions 4.0.155.5 et ultérieures du WLC, bien que la version 4.0.206.0 offre des performances optimales avec MFP. Le client MFP est pris en charge sur la version 4.1.171.0 et les versions ultérieures.

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.

Informations générales

Dans 802.11, les trames de gestion telles que (de)authentication, (dis)association, beacons et sones sont toujours non authentifiées et non chiffrées. En d'autres termes, les trames de gestion 802.11 sont toujours envoyées de manière non sécurisée, contrairement au trafic de données, qui sont cryptées avec des protocoles tels que WPA, WPA2 ou, du moins, WEP, etc.

Cela permet à un attaquant d'usurper une trame de gestion du point d'accès pour attaquer un client associé à un point d'accès. Avec les trames de gestion usurpées, un pirate peut effectuer ces actions :

- Exécuter un déni de service (DOS) sur le WLAN
- Tentez une attaque de type Man in the Middle sur le client lors de sa reconnexion
- Exécuter une attaque de dictionnaire hors connexion

La MFP surmonte ces pièges lorsqu'elle authentifie les trames de gestion 802.11 échangées dans l'infrastructure de réseau sans fil.

Remarque : Ce document est axé sur **l'infrastructure et le MFP client**.

Remarque : certaines restrictions s'appliquent à certains clients sans fil pour communiquer avec des périphériques d'infrastructure compatibles MFP. La MFP ajoute un long ensemble d'éléments d'information à chaque requête de sonde ou balise SSID. Certains clients sans fil tels que les assistants numériques personnels, les smartphones, les scanners à codes barres, etc., ont une mémoire et un processeur limités. Vous ne pouvez donc pas traiter ces requêtes ou balises. Par conséquent, vous ne voyez pas entièrement le SSID, ou vous ne pouvez pas vous associer à ces périphériques d'infrastructure, en raison d'une mauvaise compréhension des capacités du SSID.

Ce problème n'est pas spécifique à MFP. Cela se produit également avec tout SSID qui a plusieurs éléments d'information (IE). Il est toujours conseillé de tester les SSID *activés* MFP sur l'environnement avec tous les types de clients disponibles avant de les déployer en temps réel.

Note:

Voici les composants du module MFP d'infrastructure :

- **Protection des trames de gestion** - Lorsque la protection des trames de gestion est activée, le point d'accès ajoute un élément MIC IE (Message Integrity Check Information) à chaque trame de gestion qu'il transmet. Toute tentative de copie, de modification ou de relecture de la trame invalide la MIC. Un point d'accès, configuré pour valider les trames MFP reçoit une trame avec une MIC non valide, la signale au WLC.
- **Validation des trames de gestion** - Lorsque la validation des trames de gestion est activée, le point d'accès valide toutes les trames de gestion qu'il reçoit des autres points d'accès du réseau. Il garantit que l'IE MIC est présente (lorsque l'émetteur est configuré pour transmettre des trames MFP) et correspond au contenu de la trame de gestion. S'il reçoit une trame qui ne contient pas d'IE MIC valide d'un BSSID qui appartient à un AP, qui est configuré pour transmettre des trames MFP, il signale la différence au système de gestion du réseau.**Remarque :** Pour que les horodatages fonctionnent correctement, tous les WLC doivent être synchronisés avec le protocole NTP (Network Time Protocol).
- **Rapports d'événements** : le point d'accès avertit le WLC lorsqu'il détecte une anomalie. Le WLC agrège les événements anormaux et les signale via des interruptions SNMP au gestionnaire de réseau.

Fonctionnalité MFP d'infrastructure

Avec MFP, toutes les trames de gestion sont cryptographiquement hachées pour créer un contrôle d'intégrité des messages (MIC). Le MIC est ajouté à la fin de la trame (avant la séquence de contrôle de trame (FCS)).

- Dans une architecture sans fil centralisée, la MFP d'infrastructure est activée/désactivée sur le WLC (configuration globale). La protection peut être désactivée de manière sélective par WLAN et la validation peut être désactivée de manière sélective par AP.
- La protection peut être désactivée sur les WLAN utilisés par les périphériques qui ne peuvent pas gérer les IE supplémentaires.
- La validation doit être désactivée sur les points d'accès surchargés ou suralimentés.

Lorsque MFP est activé sur un ou plusieurs WLAN configurés dans le WLC, le WLC envoie une clé unique à chaque radio sur chaque AP enregistré. Les trames de gestion sont envoyées par le point d'accès sur les WLAN MFP. Ces points d'accès sont étiquetés avec une IE MIC de protection de trame. Toute tentative de modification de la trame invalide le message, ce qui fait que le point d'accès récepteur configuré pour détecter les trames MFP signale la différence au contrôleur WLAN.

Il s'agit d'un processus étape par étape de MFP, mis en oeuvre dans un environnement d'itinérance :

1. Avec MFP globalement activé, le WLC génère une clé unique pour chaque point d'accès / WLAN configuré pour MFP. Les WLC communiquent en eux-mêmes pour que tous les WLC

connaissent les clés de tous les AP/BSS d'un domaine de mobilité.**Remarque :** Tous les contrôleurs d'un groupe de mobilité/RF doivent avoir une MFP configurée de manière identique.
2. Lorsqu'un point d'accès reçoit une trame protégée MFP pour un BSS qu'il ne connaît pas, il met en mémoire tampon une copie de la trame et interroge le WLC pour obtenir la clé.
3. Si le BSSID n'est pas connu sur le WLC, il renvoie le message “ Unknown BSSID ” à l'AP, et l'AP abandonne les trames de gestion reçues de ce BSSID.
4. Si le BSSID est connu sur le WLC, mais que la MFP est désactivée sur ce BSSID, le WLC renvoie un BSSID “ désactivé. ” L'AP suppose alors que toutes les trames de gestion reçues de ce BSSID n'ont pas de MIC MFP.
5. Si le BSSID est connu et que la MFP est activée, le WLC renvoie la clé MFP au point d'accès demandeur (via le tunnel de gestion LWAPP crypté AES).
6. Le point d'accès met en cache les clés reçues de cette manière. Cette clé est utilisée pour valider ou ajouter MIC IE.

Fonctionnalité MFP du client

Le client MFP protège les clients authentifiés contre les trames usurpées, ce qui empêche l'efficacité de nombreuses attaques courantes contre les réseaux locaux sans fil. La plupart des attaques, telles que les attaques de déauthentification, reviennent simplement à des performances dégradées lorsqu'elles se heurtent à des clients valides.

Plus précisément, le client MFP chiffre les trames de gestion envoyées entre les points d'accès et les clients CCXv5 afin que les points d'accès et les clients puissent prendre des mesures préventives et abandonner les trames de gestion de classe 3 usurpées (c'est-à-dire les trames de gestion transmises entre un point d'accès et un client authentifié et associé). La MFP client exploite les mécanismes de sécurité définis par la norme IEEE 802.11i pour protéger les types de trames de gestion de monodiffusion de classe 3 : action de désassociation, de déauthentification et de QoS (WMM). La MFP client peut protéger une session de point d'accès client contre le type d'attaque de déni de service le plus courant. Il protège les trames de gestion de classe 3 avec la même méthode de chiffrement utilisée pour les trames de données de la session. Si une trame reçue par le point d'accès ou le client échoue au déchiffrement, elle est abandonnée et l'événement est signalé au contrôleur.

Pour utiliser la MFP du client, les clients doivent prendre en charge la MFP CCXv5 et négocier WPA2 avec TKIP ou AES-CCMP. EAP ou PSK peut être utilisé pour obtenir la PMK. La gestion de la mobilité des contrôleurs et CCKM permet de distribuer les clés de session entre les points d'accès ou l'itinérance rapide des couches 2 et 3.

Afin d'empêcher les attaques contre les trames de diffusion, les points d'accès qui prennent en charge CCXv5 n'émettent aucune trame de gestion de classe de diffusion 3 (comme la dissociation, la déauthentification ou l'action). Les clients CCXv5 et les points d'accès doivent ignorer les trames de gestion de classe de diffusion 3.

Le MFP client complète le MFP d'infrastructure au lieu de le remplacer, car le MFP d'infrastructure continue de détecter et de signaler les trames de monodiffusion non valides envoyées aux clients qui ne sont pas compatibles client-MFP, ainsi que les trames de gestion de classe 1 et 2 non valides. Le MFP d'infrastructure est appliqué uniquement aux trames de gestion qui ne sont pas protégées par le MFP client.

Composants MFP client

Le MFP client se compose des composants suivants :

- Génération et distribution de clés
- Protection et validation des trames de gestion
- Rapports d'erreurs

Génération et distribution de clés

Le MFP client n'utilise pas les mécanismes de génération et de distribution de clés qui ont été dérivés pour le MFP d'infrastructure. Au lieu de cela, le client MFP utilise les mécanismes de sécurité définis par la norme IEEE 802.11i pour protéger également les trames de gestion de monodiffusion de classe 3. Les stations doivent prendre en charge CCXv5 et négocier TKIP ou AES-CCMP pour utiliser la MFP client. EAP ou PSK peut être utilisé pour obtenir la PMK.

Protection des trames de gestion

Les trames de gestion de classe 3 de monodiffusion sont protégées par l'application d'AES-CCMP ou de TKIP de la même manière que celles déjà utilisées pour les trames de données. Des parties de l'en-tête de trame sont copiées dans le composant de charge utile chiffré de chaque trame pour une protection supplémentaire, comme indiqué dans les sections suivantes.

Ces types de trame sont protégés :

- Dissociation
- Déauthentification
- Trames d'action QoS (WMM)

Les trames de données protégées AES-CCMP et TKIP incluent un compteur de séquence dans les champs IV, qui est utilisé pour empêcher la détection de relecture. Le compteur de transmission actuel est utilisé pour les trames de données et de gestion, mais un nouveau compteur de réception est utilisé pour les trames de gestion. Les compteurs de réception sont testés pour s’assurer que chaque trame a un numéro supérieur à la dernière trame reçue (afin de s’assurer que les trames sont uniques et n’ont pas été relayées). Il n’est donc pas important que ce schéma fasse que les valeurs reçues ne soient pas séquentielles.

Rapports d'erreurs

Les mécanismes de rapport MFP-1 sont utilisés pour signaler les erreurs de désencapsulation de trame de gestion détectées par les points d’accès. Autrement dit, le WLC collecte des statistiques d'erreur de validation MFP et transmet périodiquement les informations collectées au WCS.

Les erreurs de violation MFP détectées par les stations clientes sont traitées par la fonction CCXv5 Roaming and Real Time Diagnostics et ne sont pas incluses dans le champ d'application de ce document.

Protection des trames de gestion de diffusion

Afin d'empêcher les attaques qui utilisent des trames de diffusion, les points d'accès qui prennent en charge CCXv5 ne transmettent aucune trame de gestion de classe de diffusion 3 (c'est-à-dire

disassoc, deauth ou action), à l'exception des trames de désauthentification/disassociation de confinement non autorisé. Les stations clientes compatibles CCXv5 doivent ignorer les trames de gestion de classe de diffusion 3. Les sessions MFP sont supposées se trouver dans un réseau correctement sécurisé (authentification forte plus TKIP ou CCMP), de sorte que l'ignorance des diffusions de confinement non autorisées ne pose pas de problème.

De même, les points d'accès rejettent les trames de gestion de diffusion entrantes. Aucune trame de gestion de diffusion entrante n'est actuellement prise en charge. Aucune modification de code n'est donc requise pour cela.

Plates-formes prises en charge

Ces plates-formes sont prises en charge :

- Contrôleurs WLAN200621064400WiSM3750 avec contrôleur 440x intégréRouteurs 26/28/37/38xx
- Points d'accès LWAPPAP 1000AP 1100, 1130AP 1200, 1240, 1250AP 1310
- Logiciel clientADU 3.6.4 et versions ultérieures
- Systèmes de gestion de réseauxWCS

Le point d'accès LWAPP maillé 1500 n'est pas pris en charge dans cette version.

Modes pris en charge

Les points d'accès LWAPP qui fonctionnent dans ces modes prennent en charge la MFP du client :

Modes de point d'accès pris en charge	
Mode	**Support MFP client**
Municipal	Oui
Monitor	Non
Snider	Non
Détecteur de virus	Non
REAP hybride	Oui
REAP	Non
Racine du pont	Oui
WGB	Non

Support de cellules mixtes

Les stations clientes qui ne sont pas compatibles CCXv5 peuvent s'associer à un WLAN MFP-2. Les points d'accès suivent les clients compatibles MFP-2 et ceux qui ne le sont pas afin de déterminer si des mesures de sécurité MFP-2 sont appliquées aux trames de gestion de monodiffusion sortantes et prévues sur les trames de gestion de monodiffusion entrantes.

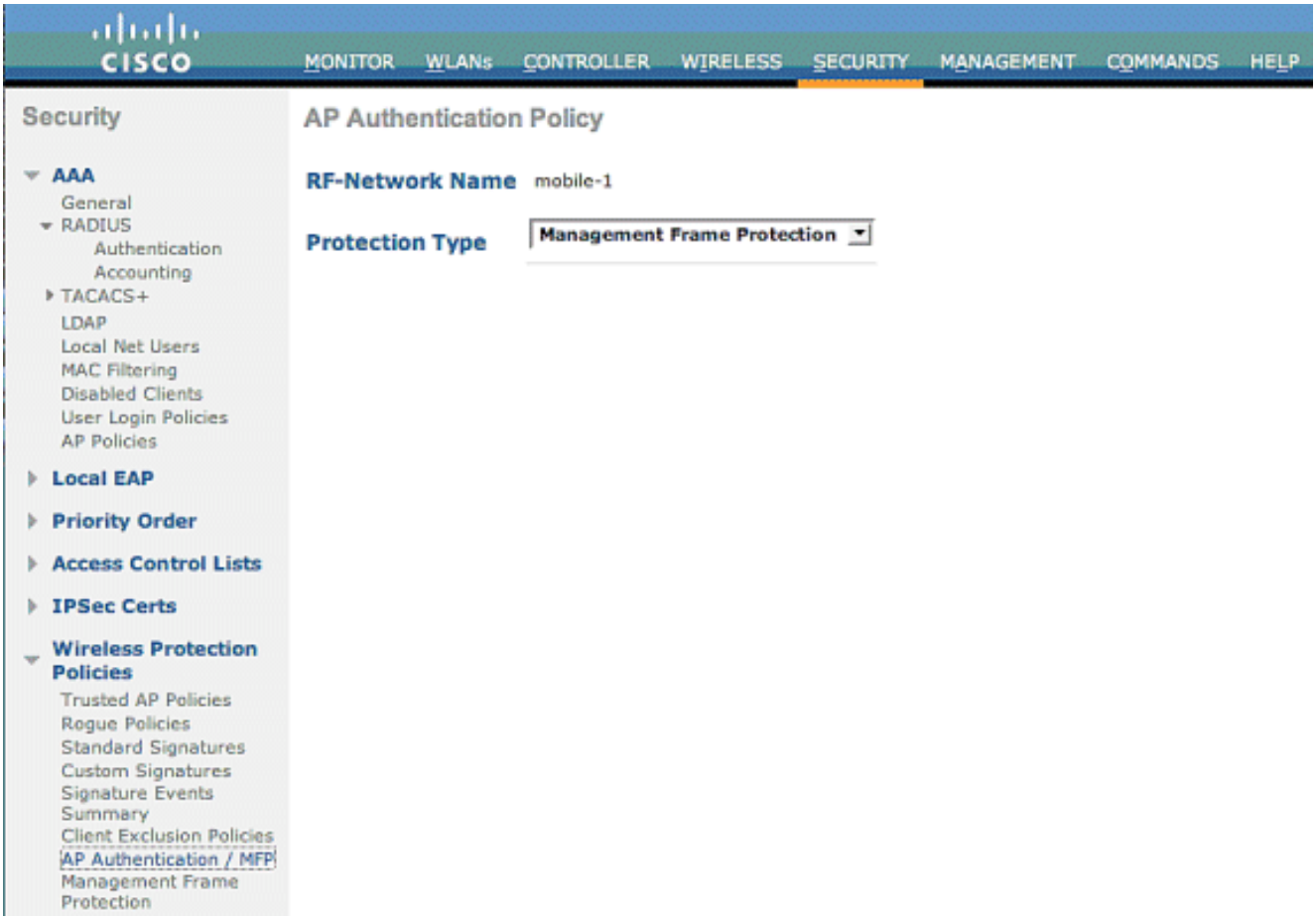
Configuration

Configuration de MFP sur un contrôleur

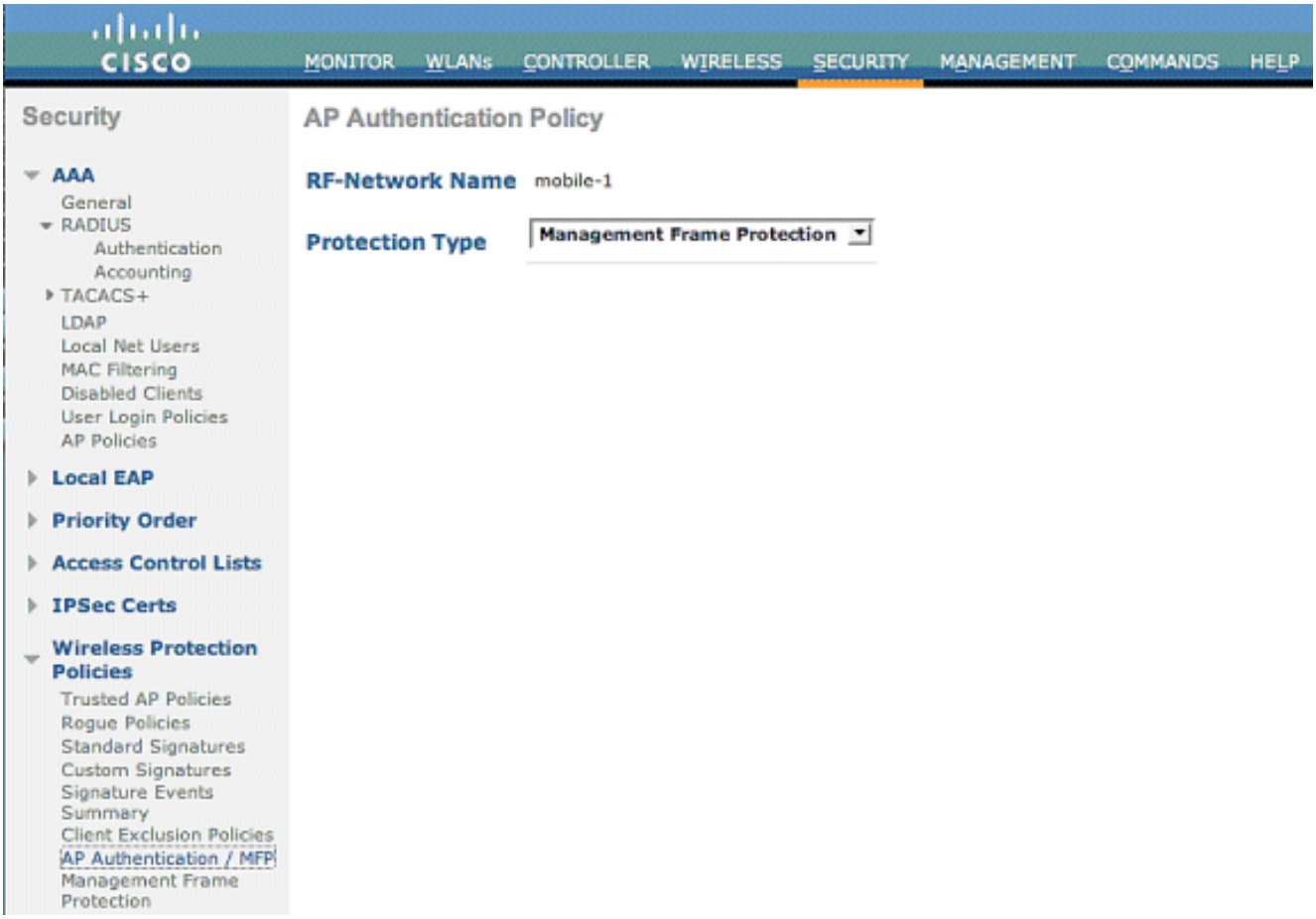
Vous pouvez configurer globalement MFP sur un contrôleur. Dans ce cas, **la protection et la validation des trames de gestion sont activées par défaut pour chaque point d'accès joint**, et l'authentification des points d'accès est automatiquement désactivée.

Procédez comme suit pour configurer la multifonction globalement sur un contrôleur.

1. Dans l'interface graphique du contrôleur, cliquez sur **Security**. Dans l'écran qui en résulte, cliquez sur **AP Authentication/MFP** sous **Wireless Protection Policies**.

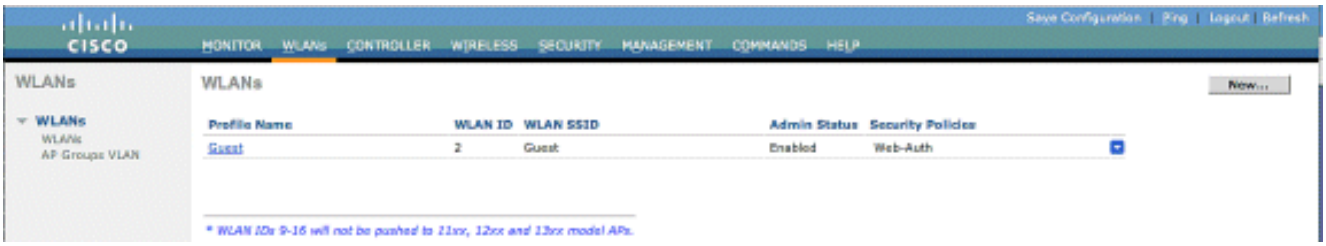


2. Dans la stratégie d'authentification AP, choisissez **Management Frame Protection** dans le menu déroulant **Protection Type** et cliquez sur **Apply**.

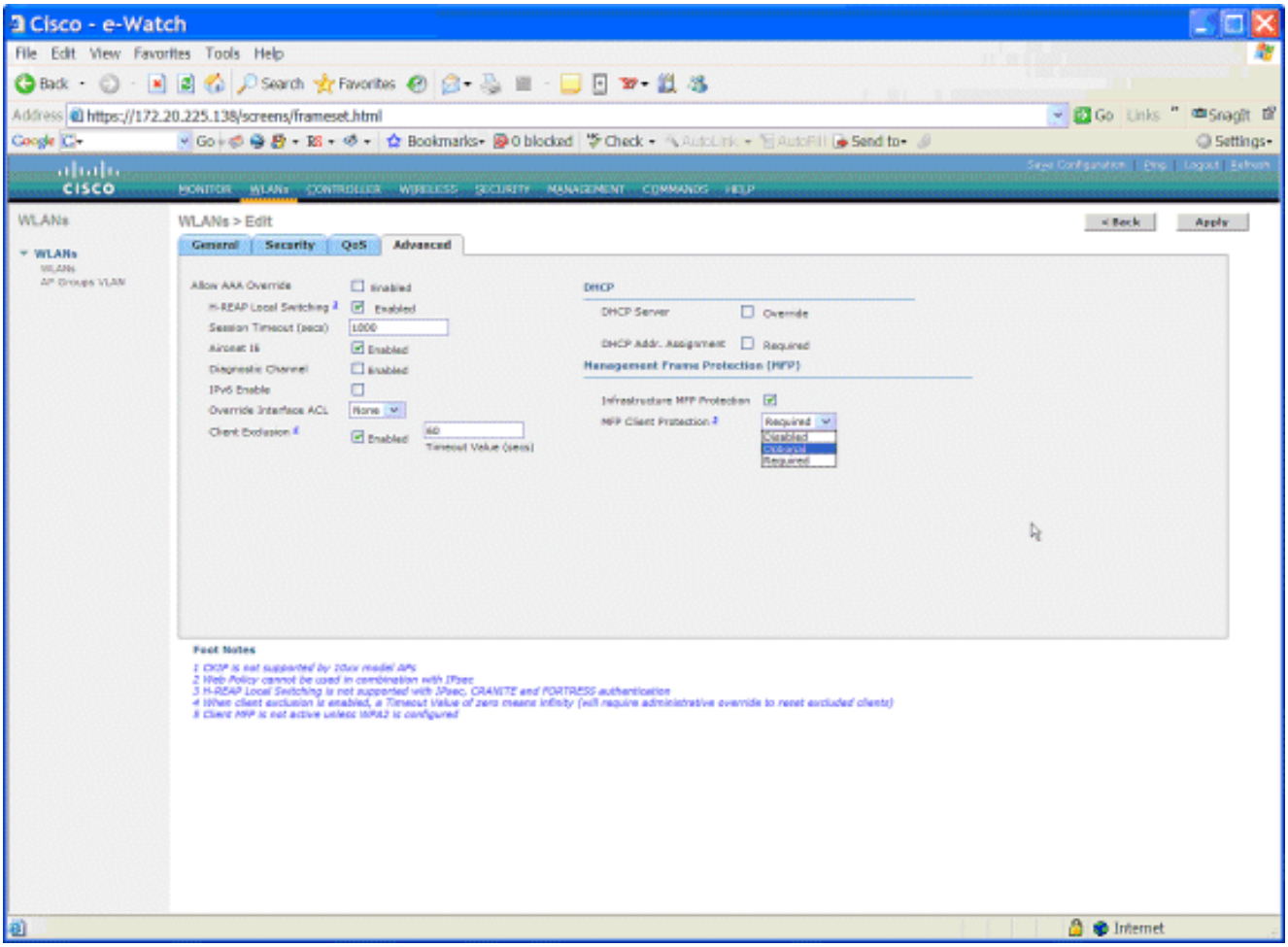


Configuration de MFP sur WLAN

Vous pouvez également activer/désactiver la protection MFP de l'infrastructure et la MFP client sur chaque WLAN configuré sur le WLC. Les deux sont activés par défaut via la protection MFP de l'infrastructure, qui est active uniquement si elle est globalement activée, et la MFP du client n'est active que si le WLAN est configuré avec la sécurité WPA2. Suivez les étapes suivantes afin d'activer MFP sur un WLAN :

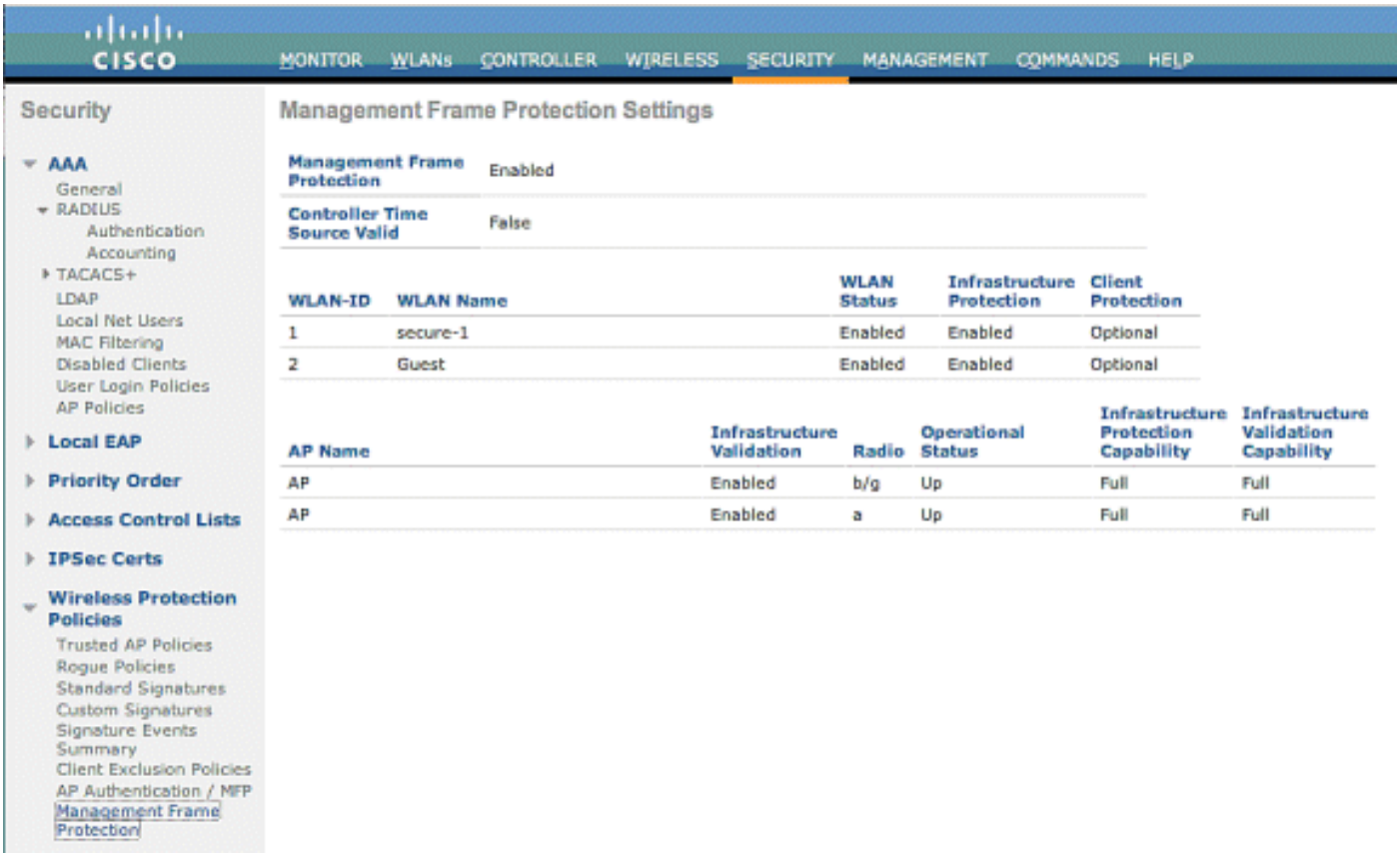
1. Dans l'interface graphique du WLC, cliquez sur **WLAN** et cliquez sur **New** afin de créer un nouveau
WLAN.


2. Sur la page de modification des WLAN, accédez à l'onglet *Advanced* et cochez la case **Infrastructure MFP Protection** pour activer l'infrastructure MFP sur ce WLAN. Afin de désactiver la protection MFP d'infrastructure pour ce WLAN, décochez cette case. Afin d'activer la fonction Client MFP, sélectionnez l'option requise ou facultative dans le menu déroulant. Si vous choisissez Client MFP= Obligatoire, assurez-vous que tous vos clients ont la prise en charge de MFP-2 ou qu'ils ne peuvent pas se connecter. Si vous choisissez facultatif, les clients MFP et non MFP peuvent se connecter sur le même
WLAN.



Vérification

Afin de vérifier les configurations MFP à partir de l'interface utilisateur graphique, cliquez sur **Management Frame Protection** sous Wireless Protection Policies à partir de la page Security. Vous accédez ainsi à la page MFP Settings.



Dans la page MFP Settings, vous pouvez voir la configuration MFP sur le WLC, le LAP et le WLAN. Voici un exemple :

- Le champ Management Frame Protection indique si MFP est activé globalement pour le WLC.
- Le champ Source de temps du contrôleur valide indique si l'heure du WLC est définie localement (par saisie manuelle de l'heure) ou via une source externe (par exemple un serveur NTP). Si l'heure est définie par une source externe, la valeur de ce champ est True. Si l'heure est définie localement, la valeur est « False ». La source temporelle est utilisée pour valider les trames de gestion entre les points d'accès de différents WLC dont la mobilité est également configurée.**Remarque :** si la MFP est activée sur tous les WLC d'un groupe de mobilité/RF, il est toujours recommandé d'utiliser un serveur NTP pour définir l'heure du WLC dans un groupe de mobilité.
- Le champ **MFP Protection** indique si MFP est activé pour les réseaux locaux sans fil individuels.
- Le champ **Validation MFP** indique si MFP est activé pour les points d'accès individuels.

Ces commandes show peuvent être utiles :

- **show wps summary** : utilisez cette commande afin de voir un résumé des stratégies de protection sans fil actuelles (qui inclut MFP) du WLC.
- **show wps mfp summary** - Afin de voir le paramètre MFP global actuel du WLC, entrez cette commande.
- **show ap config general** *AP_name* - Afin de voir l'état MFP actuel pour un point d'accès particulier, entrez cette commande.

Voici un exemple de la sortie de la commande **show ap config general** *AP_name :*

```
(Cisco Controller) >show ap config general AP
```

```
Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 29
MAC Address...................................... 00:19:2f:7e:3a:30
IP Address Configuration......................... DHCP
IP Address....................................... 172.20.225.142
IP NetMask....................................... 255.255.255.248
Gateway IP Addr.................................. 172.20.225.137
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch.............................
Secondary Cisco Switch..........................
Tertiary Cisco Switch...........................
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... H-Reap
Public Safety ................................... Global: Disabled, Local: Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.169.24
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070414:021809)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3QX
AP Certificate Type.............................. Manufacture Installed
H-REAP Vlan mode :............................... Disabled
Management Frame Protection Validation........... Enabled
Console Login Name..............................
Console Login State.............................. Unknown
Ethernet Port Duplex............................. Auto
Ethernet Port Speed.............................. Auto
```

Voici un exemple du résultat de la commande **show wps mfp summary** :

```
(Cisco Controller) >show wps mfp summary

Global MFP state................................ enabled
Controller Time Source Valid.................... false


                                  WLAN       Infra.      Client
WLAN ID  WLAN Name                Status     Protection  Protection
-------  -------------------------  ---------  ----------  ----------
1        secure-1                  Enabled    Enabled     Optional
2        Guest                     Enabled    Enabled     Optional but inactive (WPA2 not
configured)
```

```
                    Infra.              Operational     --Infra. Capability--
AP Name             Validation  Radio   State           Protection  Validation
------------------  ----------  -----   --------------  ----------  ----------
AP                  Enabled     b/g     Up              Full        Full
```

Ces commandes debug peuvent être utiles ;

- **debug wps mfp lwapp** - Affiche les informations de débogage des messages MFP.
- **debug wps mfp detail** - Affiche des informations de débogage détaillées pour les messages MFP.
- **debug wps mfp report** - Affiche les informations de débogage pour les rapports MFP.
- **debug wps mfp mm** - Affiche les informations de débogage pour les messages de mobilité MFP (inter-contrôleur).

Remarque : Il existe également plusieurs sniffeurs de paquets sans fil gratuits disponibles sur Internet, qui peuvent être utilisés pour capturer et analyser les trames de gestion 802.11. Par exemple, les sniffeurs de paquets sont Omnipeek et Wireshark.

Informations connexes

- Configuration des solutions de sécurité : Guide de configuration WLC
- Configuration des solutions de sécurité dans WCS
- Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)
- Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Exemple de configuration d'une affectation de VLAN dynamique avec un serveur RADIUS et un contrôleur de réseau local sans fil
- Cisco Secure Services Client avec authentification EAP-FAST
- FAQ sur WLC
- Page de prise en charge du mode sans fil
- Support 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.