Détection de systèmes indésirables sous des réseaux sans fil unifiés

Contenu

Introduction

Les réseaux sans fil étendent les réseaux filaires et augmentent la productivité des travailleurs et l'accès aux informations. Cependant, un réseau sans fil non autorisé représente un souci supplémentaire de couche de sécurité. La sécurité du port sur les réseaux filaires est moins mise de l'avant, et les réseaux sans fil sont une extension facile aux réseaux filaires. Par conséquent, un employé qui amène son propre point d'accès Cisco (AP) dans une infrastructure sans fil bien-sécurisée ou une infrastructure filaire et permet l'accès d'utilisateurs non autorisés à ce réseau autrement sécurisé peut facilement compromettre un réseau sécurisé.

La détection des anomalies permet à l'administrateur réseau de surveiller et d'éliminer ce problème de sécurité. L'architecture réseau unifiée de Cisco fournit deux méthodes de détection des pirates qui permettent une solution complète d'identification et de confinement des pirates sans avoir besoin de réseaux et d'outils de superposition coûteux et difficiles à justifier.

Présentation des fonctionnalités

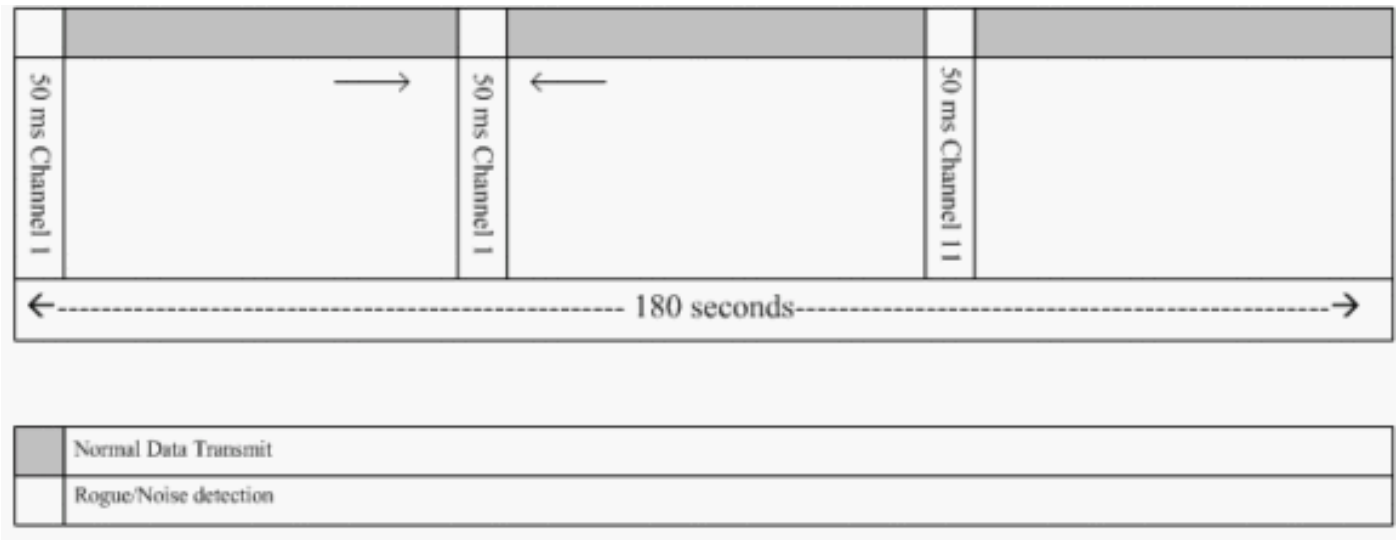
La détection des fraudes n'est soumise à aucune réglementation et aucune conformité légale n'est requise pour son fonctionnement. Cependant, le confinement des pirates introduit généralement des problèmes juridiques qui peuvent mettre le fournisseur d'infrastructure dans une position inconfortable s'il est laissé fonctionner automatiquement. Cisco est extrêmement sensible à ces problèmes et fournit ces solutions. Chaque contrôleur est configuré avec un nom de groupe RF.Une fois qu'un point d'accès léger s'enregistre auprès d'un contrôleur, il intègre un **élément d'information d'authentification (IE)** qui est spécifique au groupe RF configuré sur le contrôleur dans toutes ses trames de réponse de balise/sonde. Lorsque le point d'accès léger entend des trames de réponse de balise/sonde d'un point d'accès sans ce point d'accès ou avec un **mauvais point d'accès**, alors le point d'accès léger signale que le point d'accès est un point d'accès non

autorisé, enregistre son BSSID dans une table non autorisé, et envoie la table au contrôleur. Il existe deux méthodes, à savoir le protocole RLDP (Rogue Location Discovery Protocol) et le fonctionnement passif, qui sont expliquées en détail ; voir la section Déterminer les liaisons actives.

Détection des failles d'infrastructure

La détection des anomalies dans un environnement sans fil actif peut être coûteuse. Ce processus demande au point d'accès en service (ou en mode local) d'arrêter le service, d'écouter le bruit et d'effectuer une détection de virus. L'administrateur réseau configure les canaux à analyser et configure la période pendant laquelle toutes les stations sont analysées. Le point d'accès écoute les balises de client non autorisé pendant 50 ms, puis retourne au canal configuré afin de servir à nouveau les clients. Cette analyse active, combinée aux messages de voisinage, identifie les points d'accès qui sont des indésirables et les points d'accès valides et qui font partie du réseau. Afin de configurer les canaux analysés et la période d'analyse, accédez à **Wireless > 802.11b/g Network** (" **b/g** " ou " **un** " selon les besoins du réseau) et sélectionnez le bouton **Auto RF** dans le coin supérieur droit de la fenêtre du navigateur.

Vous pouvez faire défiler jusqu'à **Canaux de surveillance du bruit/des interférences/des anomalies** afin de configurer les canaux à analyser pour détecter les algues et le bruit. Les options disponibles sont les suivantes : Tous les canaux (1 à 14), les canaux de pays (1 à 11) ou les canaux DCA (Dynamic Channel Association) (par défaut 1, 6 et 11). La période d'analyse via ces canaux peut être configurée dans la même fenêtre, sous **Intervalles de surveillance (60 à 3600 secondes)** avec l'intervalle de mesure du bruit. Par défaut, l'intervalle d'écoute pour le bruit et les rogues hors canal est de 180 secondes. Cela signifie que chaque canal est analysé toutes les 180 secondes. Voici un exemple des canaux DCA qui sont analysés toutes les 180 secondes :



Comme illustré, un grand nombre de canaux configurés pour être analysés combinés avec les intervalles d'analyse courts, laisse moins de temps au point d'accès pour traiter réellement les clients de données.

Le point d'accès léger attend pour étiqueter les clients et les points d'accès comme des rogues parce que ces rogues ne sont probablement pas signalés par un autre point d'accès avant qu'un autre cycle ne soit terminé. Le même AP se déplace à nouveau sur le même canal afin de surveiller les AP et les clients non autorisés, ainsi que le bruit et les interférences. Si les mêmes clients et/ou points d'accès sont détectés, ils sont de nouveau répertoriés en tant que rogues sur le contrôleur. Le contrôleur commence maintenant à déterminer si ces rogues sont reliées au

réseau local ou simplement à un point d'accès voisin. Dans les deux cas, un point d'accès qui ne fait pas partie du réseau local sans fil géré est considéré comme non autorisé.

Détails de la fraude

Un point d'accès léger s'éteint hors canal pendant 50 ms afin d'écouter les clients indésirables, de surveiller le bruit et les interférences de canal. Tous les clients ou points d'accès non autorisés détectés sont envoyés au contrôleur, qui collecte ces informations :

- Adresse MAC de l'AP non autorisé
- Nom de l'AP non autorisé
- Adresse MAC du ou des clients connectés non autorisés
- Si les trames sont protégées par WPA ou WEP
- Le préambule
- Le rapport signal/bruit (SNR)
- Indicateur de puissance du signal du récepteur (RSSI)

Point d'accès Détecteur de Rogue

Vous pouvez faire fonctionner un point d'accès comme un détecteur de roubles, ce qui permet de le placer sur un port d'agrégation pour qu'il puisse entendre tous les VLAN connectés côté câblé. Il recherche ensuite le client sur le sous-réseau câblé sur tous les VLAN. Le point d'accès du détecteur de non-respect écoute les paquets ARP (Address Resolution Protocol) afin de déterminer les adresses de couche 2 des clients non autorisés ou des points d'accès non autorisés identifiés envoyés par le contrôleur. Si une adresse de couche 2 correspondant est trouvée, le contrôleur génère une alarme qui identifie le point d'accès ou le client non autorisé comme une menace. Cette alarme indique que le pirate a été détecté sur le réseau câblé.

Déterminer les liaisons actives

Les points d'accès indésirables doivent être “ vus ” deux fois avant d'être ajoutés comme indésirables par le contrôleur. Les points d’accès indésirables ne sont pas considérés comme une menace s’ils ne sont pas connectés au segment filaire du réseau d’entreprise. Afin de déterminer si le pirate est actif, différentes approches sont utilisées. Ces approches incluent le RLDP.

Protocole RLDP (Rogue Location Discovery Protocol)

RLDP est une approche active, qui est utilisée lorsque le point d'accès non autorisé n'a aucune authentification (authentification ouverte) configurée. Ce mode, qui est désactivé par défaut, demande à un AP actif de se déplacer vers le canal non autorisé et de se connecter à ce dernier en tant que client. Pendant ce temps, le point d'accès actif envoie des messages de déauthentification à tous les clients connectés, puis arrête l'interface radio. Ensuite, il s'associera au point d'accès non autorisé en tant que client.

Le point d'accès tente ensuite d'obtenir une adresse IP du point d'accès non autorisé et transfère un paquet UDP (User Datagram Protocol) (port 6352) qui contient l'AP local et les informations de connexion non autorisée au contrôleur via le point d'accès non autorisé. Si le contrôleur reçoit ce paquet, l'alarme est configurée pour avertir l'administrateur réseau qu'un point d'accès non autorisé a été découvert sur le réseau câblé avec la fonctionnalité RLDP.

Remarque : utilisez la commande **debug dot11 rldp enable** afin de vérifier si le point d'accès léger s'associe et reçoit une adresse DHCP du point d'accès non autorisé. Cette commande affiche également le paquet UDP envoyé par l'AP léger au contrôleur.

Un exemple de paquet UDP (port de destination 6352) envoyé par le point d'accès léger est présenté ici :

```
0020 0a 01 01 0d 0a 01 .......(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
......x......... 0040 00 00 00 00 00 00 00 00 00 00 00 00
```

Les 5 premiers octets des données contiennent l'adresse DHCP donnée au point d'accès en mode local par le point d'accès non autorisé. Les 5 octets suivants sont l'adresse IP du contrôleur, suivie de 6 octets qui représentent l'adresse MAC du point d'accès non autorisé. Ensuite, il y a 18 octets de zéros.

Opération passive :

Cette approche est utilisée lorsque le point d'accès non autorisé a une forme d'authentification, WEP ou WPA. Lorsqu'une forme d'authentification est configurée sur un point d'accès non autorisé, le point d'accès léger ne peut pas s'associer, car il ne connaît pas la clé configurée sur le point d'accès non autorisé. Le processus commence avec le contrôleur lorsqu'il passe sur la liste des adresses MAC de client non autorisé à un point d'accès configuré comme détecteur non autorisé. Le détecteur de rouages indésirables analyse tous les sous-réseaux connectés et configurés pour les requêtes ARP, et le protocole ARP recherche une adresse de couche 2 correspondante. Si une correspondance est détectée, le contrôleur avertit l'administrateur réseau qu'un pirate est détecté sur le sous-réseau câblé.

Confinement des indésirables actif

Une fois qu'un client non autorisé est détecté sur le réseau câblé, l'administrateur réseau peut contenir à la fois le point d'accès non autorisé et les clients non autorisés. Cela peut être réalisé parce que les paquets de désauthentification 802.11 sont envoyés aux clients qui sont associés aux AP non autorisés afin que la menace que crée un tel trou soit atténuée. Chaque fois qu'il y a une tentative de contenir le point d'accès non autorisé, près de 15 % de la ressource du point d'accès léger est utilisée. Par conséquent, il est conseillé de localiser et de supprimer physiquement le point d'accès non autorisé une fois qu'il est contenu.

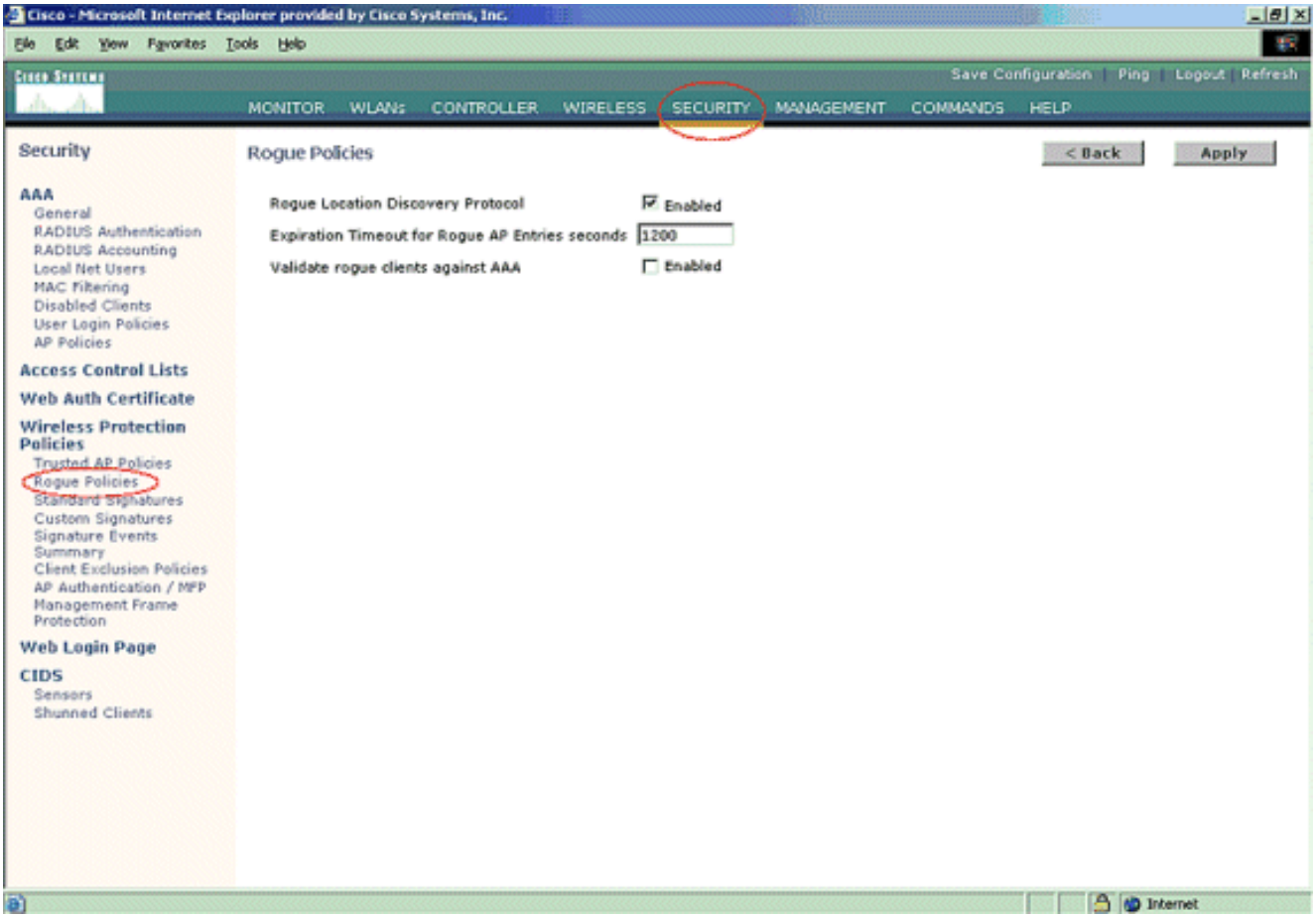
Note : À partir de la version 5.2.157.0 du WLC, une fois le rouge détecté, vous pouvez maintenant choisir de contenir manuellement ou automatiquement le code non autorisé détecté. Dans les versions logicielles du contrôleur antérieures à la version 5.2.157.0, le confinement manuel est la seule option.

Détection des anomalies - Étapes de configuration

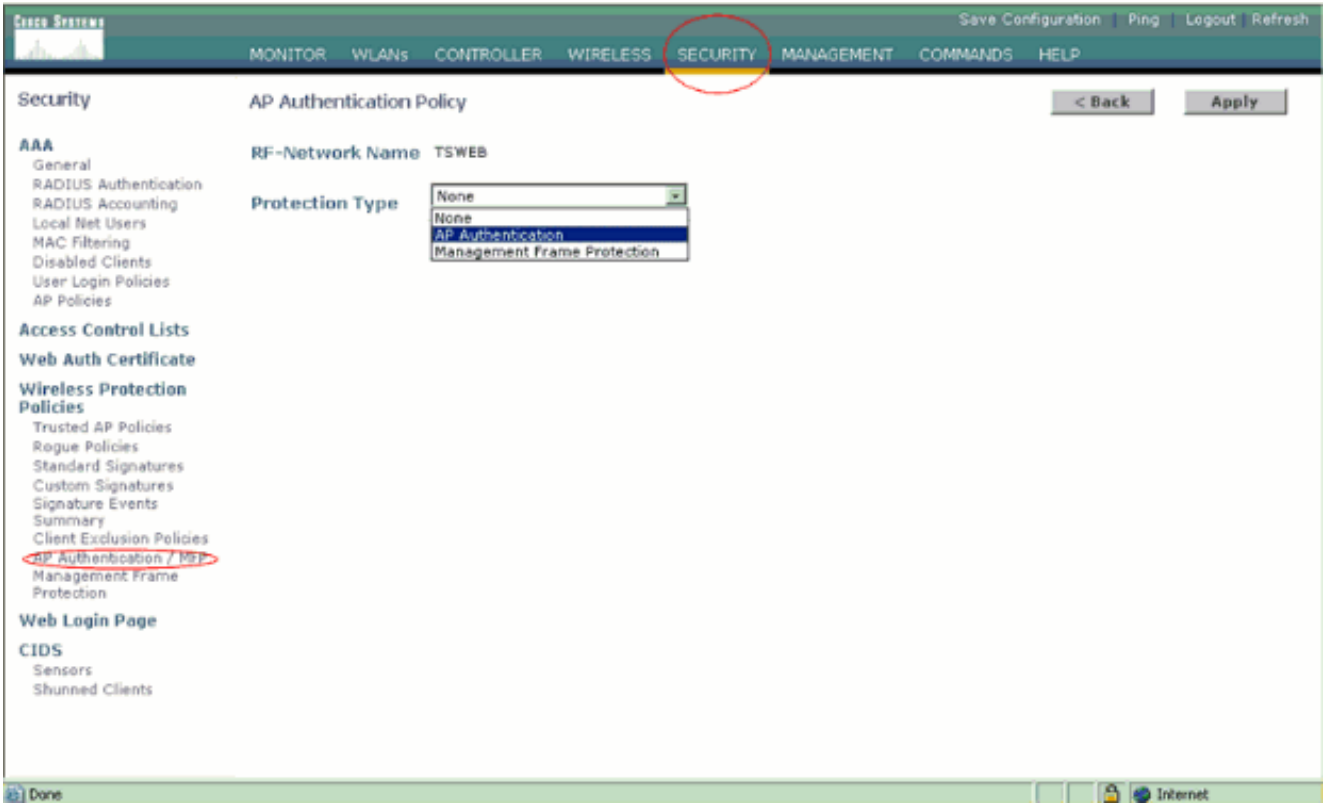
La quasi-totalité de la configuration de détection de virus est activée par défaut pour permettre une sécurité réseau optimale et prête à l'emploi. Ces étapes de configuration supposent qu'aucune détection d'infractions n'est configurée sur le contrôleur afin de clarifier des informations importantes de détection d'infractions.

Afin de configurer la détection de virus, procédez comme suit :

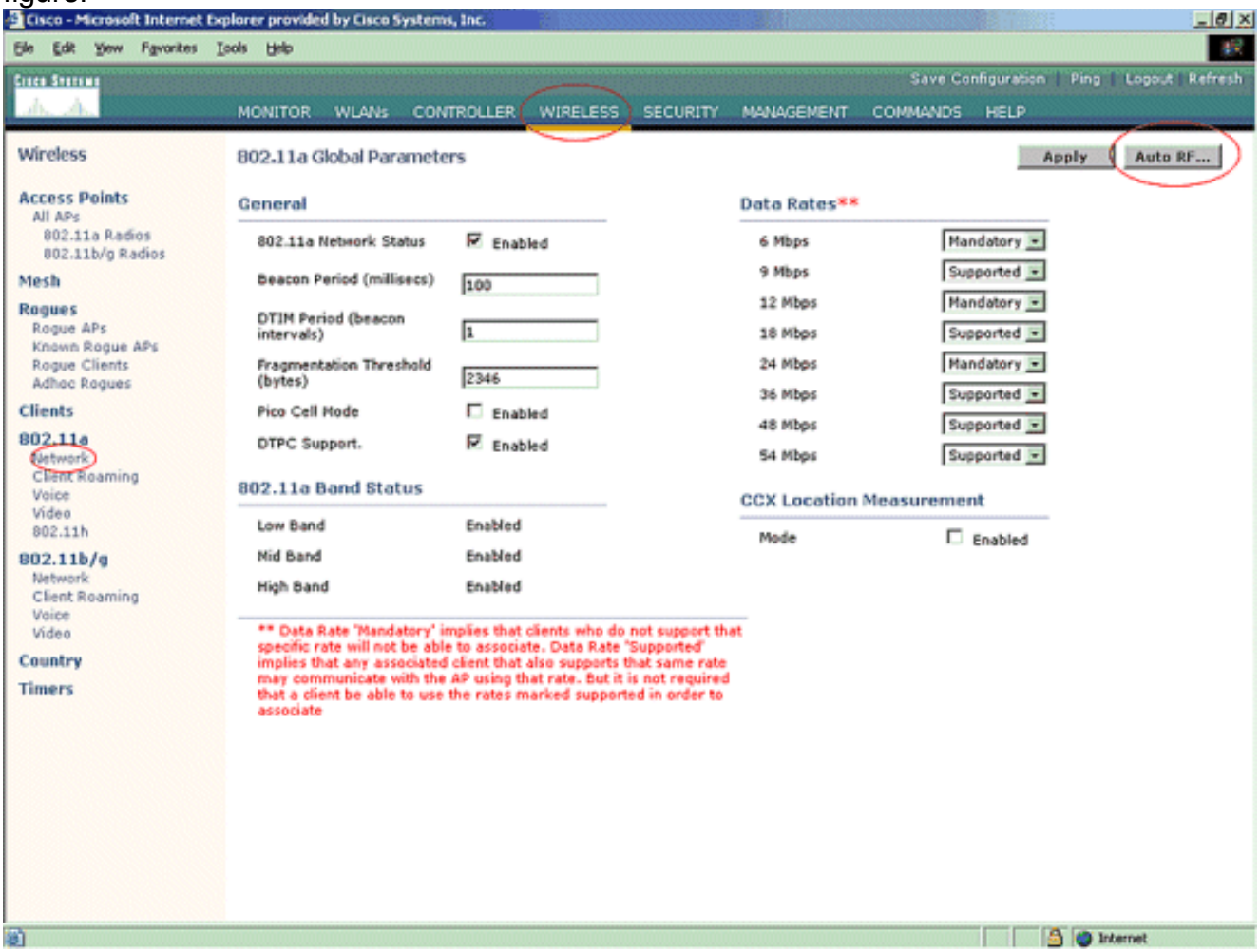
1. Assurez-vous que le protocole Détection des emplacements indésirables est activé. Afin de l'activer, choisissez **Security > Rogue Policies** et cliquez sur **Enabled** sur le **Rogue Location Discovery Protocol** comme illustré dans la figure.**Note :** Si un AP non autorisé n'est pas entendu pendant un certain temps, il est supprimé du contrôleur. Il s'agit du **délai d'expiration** d'un AP non autorisé, qui est configuré sous l'option
RLDP.



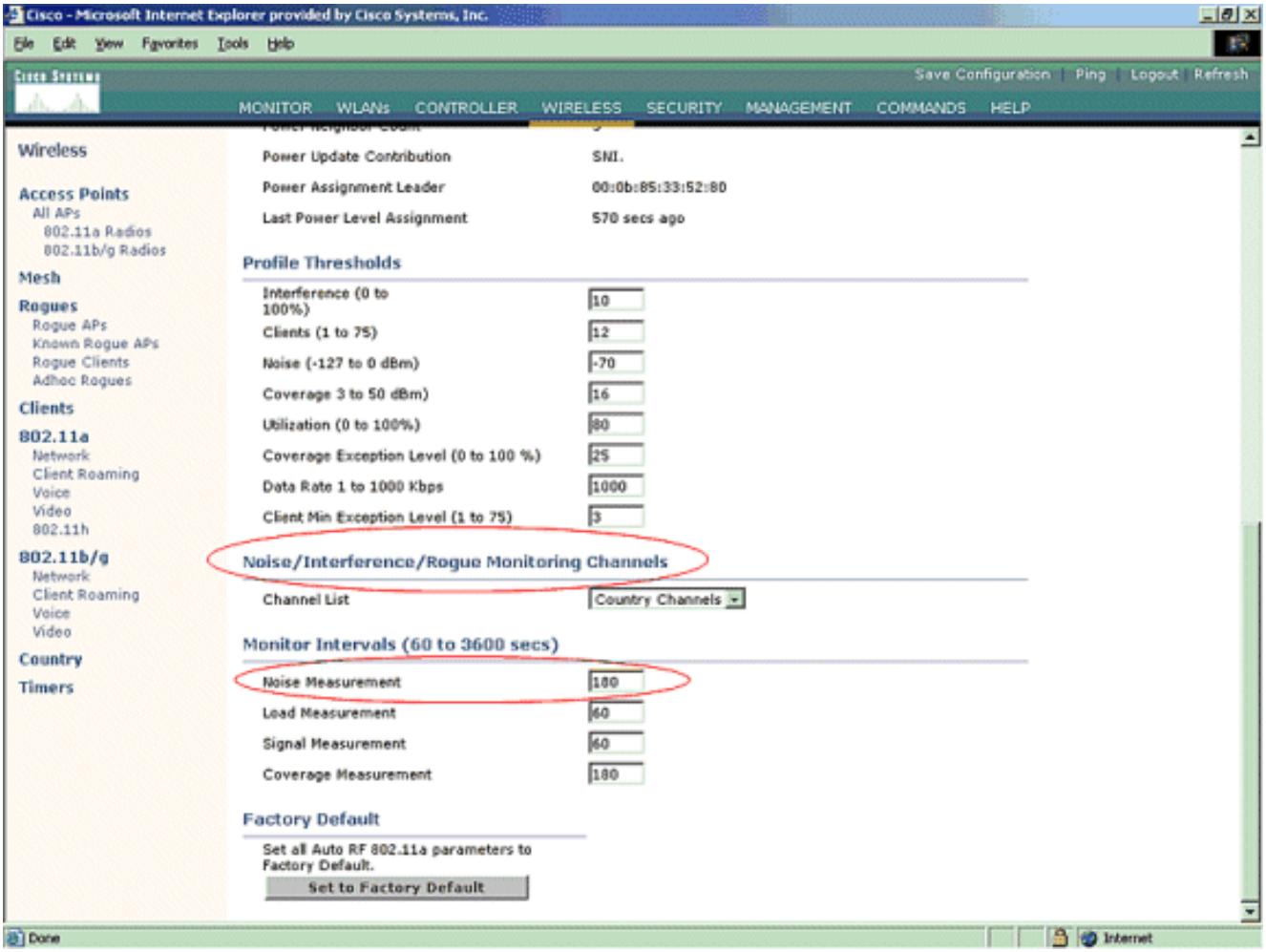
2. Il s'agit d'une étape facultative. Lorsque cette fonctionnalité est activée, les points d'accès qui envoient des paquets de voisinage RRM avec différents noms de **groupe RF** sont signalés en tant que rogues. Cela vous aidera à étudier votre environnement RF. Afin de l'activer, choisissez **Security-> AP Authentication**. Ensuite, choisissez **AP Authentication** comme Type de protection comme indiqué dans la
figure.



3. Vérifiez les canaux à analyser dans les étapes suivantes :Sélectionnez **Wireless > 802.11a Network**, puis **Auto RF** dans la partie droite comme illustré dans la figure.



Sur la page **Auto RF**, faites défiler la page vers le bas et sélectionnez **Bruit/Interférence/Rogue Monitoring Channels (Canaux de surveillance des perturbations/perturbations)**.



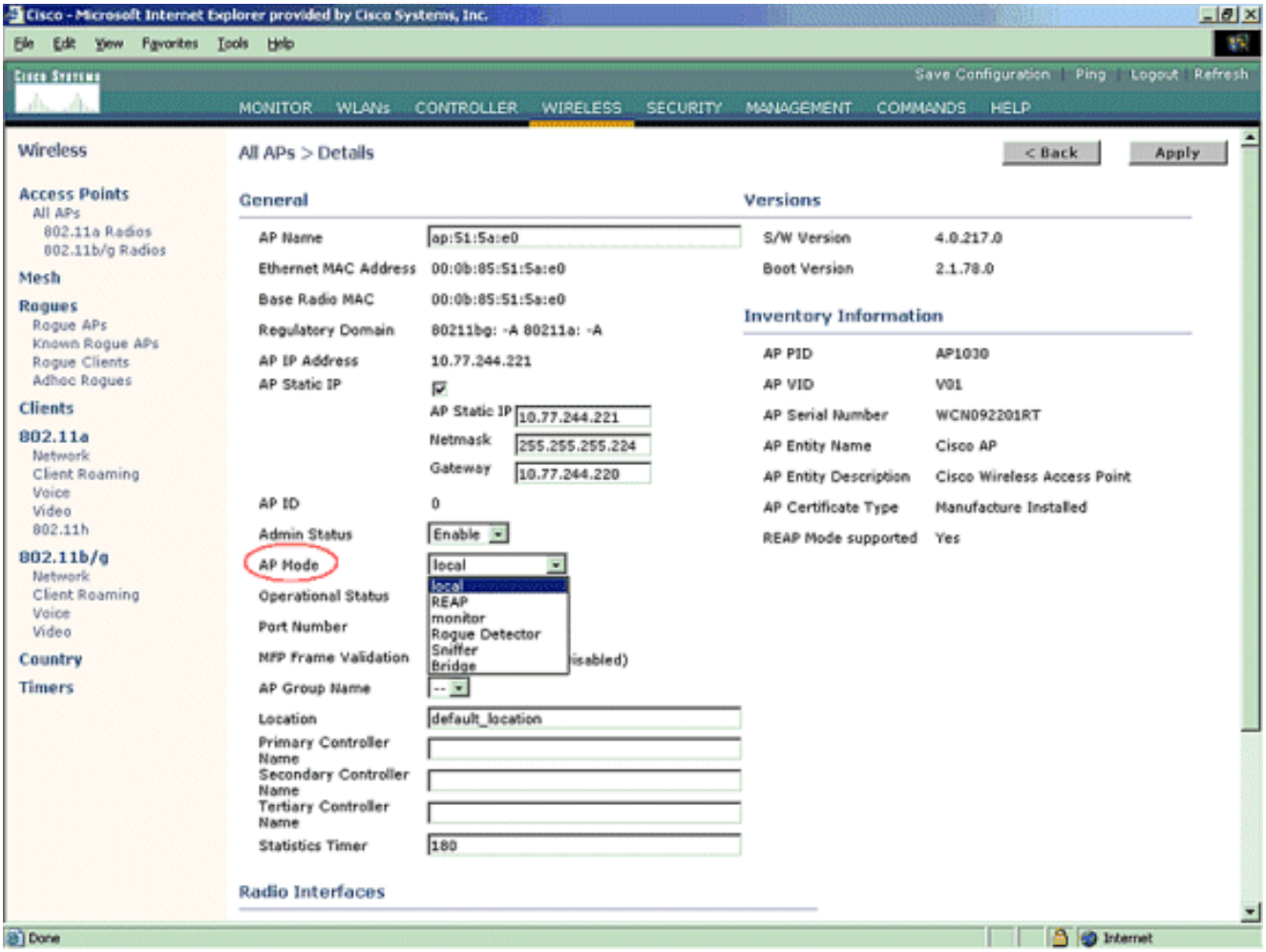
La liste des canaux détaille les canaux à analyser pour la surveillance des indésirables, en plus d'autres fonctions de contrôleur et d'AP. Référez-vous à la FAQ relative aux points d'accès légers pour plus d'informations sur les points d'accès légers et à la FAQ relative au dépannage des contrôleurs de réseau local sans fil (WLC) pour plus d'informations sur les contrôleurs sans fil.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Définissez la période d'analyse des canaux sélectionnés :La durée d'analyse du groupe de canaux défini est configurée sous **Intervalles de surveillance > Mesure du bruit**, et la plage autorisée est comprise entre 60 et 3 600 secondes. Si la valeur par défaut est de 180 secondes, les points d'accès analysent chaque canal du groupe de canaux une fois, pendant 50 ms, toutes les 180 secondes. Au cours de cette période, la radio AP passe de son canal de service au canal spécifié, écoute et enregistre les valeurs pendant une période de 50 ms, puis retourne au canal d'origine. Le temps de saut plus le temps de dwell de 50 ms fait passer le point d'accès hors canal pour environ 60 ms à chaque fois. Cela signifie que

chaque point d'accès passe environ 840 ms sur le total de 180 secondes à écouter des rogues.Impossible de modifier le ” d'écoute “ ou l'heure ” du “ et il n'est pas modifié par un ajustement de la valeur de mesure du bruit. Si le compteur de mesure du bruit est réduit, le processus de détection de voyous risque de trouver plus de voyous et de les trouver plus rapidement. Cependant, cette amélioration se fait au détriment de l'intégrité des données et du service client. Par contre, une valeur plus élevée permet une meilleure intégrité des données, mais réduit la capacité à trouver rapidement des indésirables.

5. Configurez le mode de fonctionnement du point d'accès :Un mode de fonctionnement de point d'accès léger définit le rôle du point d'accès. Les modes associés aux informations présentées dans ce document sont les suivants :**Local** : il s'agit du fonctionnement normal d'un point d'accès. Ce mode permet de traiter les clients de données pendant que les canaux configurés sont analysés pour détecter les bruits et les erreurs. Dans ce mode de fonctionnement, le point d'accès sort du canal pendant 50 ms et écoute les erreurs. Il effectue un cycle sur chaque canal, un par un, pour la période spécifiée dans la configuration RF automatique.**Surveillance** - Il s'agit du mode de réception radio uniquement, qui permet au point d'accès d'analyser tous les canaux configurés toutes les 12 secondes. Seuls les paquets de désauthentification sont envoyés dans l'air avec un point d'accès configuré de cette manière. Un point d'accès en mode de surveillance peut détecter des rogues, mais il ne peut pas se connecter à un pirate suspect en tant que client afin d'envoyer les paquets RLDP.**Remarque :** DCA fait référence aux canaux qui ne se chevauchent pas et qui sont configurables avec les modes par défaut.**Détecteur de non-respect** - Dans ce mode, la radio AP est désactivée et le point d'accès écoute le trafic filaire uniquement. Le contrôleur transmet les points d'accès configurés en tant que détecteurs indésirables, ainsi que les listes de clients indésirables suspectés et les adresses MAC des points d'accès. Le détecteur de rouages non autorisés écoute uniquement les paquets ARP et peut être connecté à tous les domaines de diffusion via une liaison agrégée si nécessaire.Vous pouvez configurer un mode AP individuel simplement, une fois que le point d'accès léger est connecté au contrôleur. Afin de changer le mode AP, connectez-vous à l'interface Web du contrôleur et accédez à **Wireless**. Cliquez sur **Details** en regard du point d'accès souhaité à afin d'afficher un écran similaire à celui-ci
   :



Utilisez le menu déroulant Mode AP afin de sélectionner le mode de fonctionnement AP souhaité.

Dépannage des commandes

Vous pouvez également utiliser ces commandes afin d'effectuer le dépannage de votre configuration sur le point d'accès :

- **show rogue ap summary** - Cette commande affiche la liste des AP non autorisés détectés par les AP légers.
- **show rogue ap detail** *<adresse MAC du point d'accès non autorisé>* - Utilisez cette commande afin d'afficher les détails d'un point d'accès non autorisé individuel. Il s'agit de la commande qui permet de déterminer si le point d'accès non autorisé est branché sur le réseau câblé.

Conclusion

La détection et le confinement des attaques au sein de la solution de contrôleur centralisé Cisco est la méthode la plus efficace et la moins intrusive du secteur. La flexibilité offerte à l'administrateur réseau permet de personnaliser l'ajustement en fonction des besoins du réseau.

Informations connexes

- Présentation des groupes RF
- Support et documentation techniques - Cisco Systems