Classification basée sur les règles dans les contrôleurs LAN sans fil (WLC) et les systèmes de contrôle sans fil (WCS)

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Classification escroc basée sur les règles
Terminologies escrocs basées sur les règles de classification
Règles escrocs de classification
Classification escroc et États voyou
États voyou expliquées
Comment configurer des règles escrocs dans WLC
Comment configurer des règles escrocs dans WCS
Informations connexes

Introduction

Dans la release 5.0 du système de contrôle sans fil (WCS), WCS a amélioré la fonction d'administration escroc pour différents types de l'escroc AP et si des règles définies par l'utilisateur de classifier automatiquement l'escroc aps. WCS a appliqué des règles escrocs de classification AP aux contrôleurs. Ce document explique la fonction d'administration escroc améliorée et les étapes nécessaires pour configurer cette fonctionnalité sur le contrôleur LAN Sans fil (WLC) et WCS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du point d'accès léger Protocol (LWAPP)
- La connaissance des solutions de sécurité Sans fil de contrôleur LAN

Composants utilisés

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

logiciel suivantes :

- Gamme Cisco 4400 WLC qui exécute les micrologiciels 5.2
- Point d'accès léger de Gamme Cisco Aironet 1130 AG (recouvrements)
- Version 5.2 de Système de contrôle sans fil Cisco

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.

Classification escroc basée sur les règles

Dans des versions WCS avant la version 5.0, WCS a affiché trop de points d'accès non autorisé (aps) dans la page **récapitulative de Sécurité**. Quoique les États voyou diffèrent, elles toutes apparaissent à une page, triée par l'adresse MAC BSSID/de l'escroc.

Dans la release WCS 5.0, WCS fonction d'administration escroc améliorée et a introduit de nouvelles terminologies (non classifié, malveillant, et amical) pour différents types de l'escroc AP et si des règles définies par l'utilisateur de classifier automatiquement l'escroc aps. WCS a appliqué des règles escrocs de classification AP aux contrôleurs.

WCS a amélioré la fonction de gestion d'État voyou pour garder l'État voyou comme *externe* une fois que l'état d'escroc a été manuellement changé à *externe*. WCS met à jour également l'état *externe* pour les autres contrôleurs quand WCS tire ou traite le message dérouté des autres contrôleurs.

Afin de prendre en charge cette caractéristique, WLC et WCS devraient exécuter la release 5.0.

Terminologies escrocs basées sur les règles de classification

Avec cette nouvelle fonctionnalité, ces nouveaux types de l'escroc AP sont introduits :

- **AP malveillant :** AP détecté qui apparie des règles malveillantes définies par l'utilisateur ou a été manuellement déplacé des aps amicaux.
- **AP amical :** Exister connu, reconnaissent, et des États voyou manquantes de confiance sont classifiées comme amicales. En outre, des aps détectés qui apparient des règles amicales définies par l'utilisateur sont classifiés comme amicaux. Des aps amicaux ne peuvent pas être contenus.
- **AP non classifié :** AP détecté qui n'a pas apparié les règles malveillantes ou amicales. AP non classifié peut être contenu. AP non classifié peut être manuellement déplacé à amical par l'utilisateur. Les règles définies par l'utilisateur de déplacer automatiquement AP non classifié à amical ou à malveillant, par exemple, sur la détection, le SSID est vide. Sur le prochain état escroc, un SSID est trouvé, et il s'avère être un SSID utilisateur-configuré.

Règles escrocs de classification

Ce sont des règles de classification applicables à chacun des types de l'escroc AP :

- Règles malveillantesLes correspondances ont géré le SSIDApparie le SSID configuré par utilisateurAucun cryptage sur un SSIDMinimum RSSIDurée de tempsNombre de clients associés
- Règles amicalesSSID géréSSID Utilisateur-configuré
- Règles non classifiéesN'apparie pas des règles malveillantes ou amicales

Parameter	Description
Time Duration (0 to 3600)	Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration field. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
Minimum RSSI (-95 to -50)	Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI field. The valid range is -95 to -50 dBm (inclusive), and the default value is 0 dBm.
Minimum number of Rogue client (1-10)	Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients field. The valid range is 1 to 10 (inclusive), and the default value is 0.
No Encryption	Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option. **Note** WCS refers to this option as "Open Authentication."
Managed SSID[1]	Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.
User configured SSID[1]	Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID field, and click **Add SSID**. You can add multiple SSIDs. To remove an SSID, select the SSID and click **Remove**.

[1]The SSID and Managed SSID conditions cannot be used with the Match All operation as these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

L'utilisateur peut choisir d'apparier **tous les,** ou **certains** conditions de règle selon chaque règle :

- **Tous les** moyens apparient toutes les conditions configurées pour la règle.
- **Tous les** moyens apparient des conditions configurées l'unes des pour la règle.
- **Certains des** moyens apparient peu des conditions configurées pour la règle

Par exemple, selon des *règles malveillantes*, l'utilisateur configure *SSID géré* et *minimum RSSI*. Puis, l'utilisateur a le choix pour apparier **tous** ou des deux conditions **l'unes des**, ou appariez juste l'état du *minimum RSSI*.

Quand le contrôleur reçoit l'état escroc, il fait ceci :

- Vérifie si AP détecté est dans la liste utilisateur-configurée de MAC. Si oui, classifiez AP comme type amical.
- Si AP détecté n'est pas dans la liste, il commence à appliquer les règles.
- D'abord, il applique des *règles malveillantes*. Si les *règles malveillantes* s'assortissent, il est

classifié comme type malveillant. Si le détecteur RLDP/rogue détermine que cet escroc est sur le réseau, il marque l'État voyou comme **menace**. L'utilisateur peut manuellement contenir AP qui change l'État voyou à **contenu**. Si AP n'est pas sur le réseau, il marque l'État voyou en tant qu'**alerte**, et l'utilisateur peut la contenir manuellement.
- Si les *règles malveillantes* ne s'assortissent pas, appliquez les *règles amicales*. Si les *règles amicales* s'assortissent, alors classifiez-le comme type amical.
- Si les *règles amicales* ne s'assortissent pas, classifiez cet AP comme non classifié. Si le détecteur RLDP/rogue détermine que cet escroc est sur le réseau, marquez l'État voyou comme **menace** et classifiez-la comme type malveillant. L'utilisateur peut manuellement contenir AP qui change l'État voyou à **contenu**. Si AP n'est pas sur le réseau, marquez l'État voyou en tant qu'**alerte**, et l'utilisateur peut la contenir manuellement.
- L'utilisateur peut manuellement déplacer AP à un type différent de classification.

Classification escroc et États voyou

Cette table affiche les différentes classifications des escrocs et des États voyou pour chaque classification.

Type basé sur les règles de classification	États voyou
AP malveillant	La menace vigilante contenue a contenu en attendant retiré
AP non classifié	L'alerte contenue a contenu en attendant retiré
AP amical	(Connu actuellement) (reconnaissez actuellement) alerte manquante interne externe interne (de disparus de confiance)

États voyou expliquées

- **En attendant —** Sur la première détection, AP détecté est mis dans l'état en attente pendant 3 minutes. Ce temps est suffisant pour que des aps gérés pour déterminer si AP détecté est un voisin AP.
- **Alerte —** Après la minuterie 3-minute, AP détecté est déplacé **pour alerter** s'il n'est pas dans la liste voisine ou liste amicale utilisateur-configurée de MAC.
- **Menace —** AP détecté est trouvé sur le réseau.
- **Contenu —** AP détecté est contenu.
- **Contenu en attendant —** AP détecté est marqué a contenu, mais l'action de retenue est retardée en raison des ressources indisponibles.
- **Interne —** AP détecté est à l'intérieur du réseau, et l'utilisateur le configure manuellement comme **amical, interne**, par exemple, les aps dans un réseau des travaux pratiques.
- **Externe —** AP détecté est en dehors du réseau, et l'utilisateur le configure manuellement comme **amical, externe**, par exemple, les aps qui appartiennent à un réseau voisin.
- **Disparus de confiance —** Si le MAC amical utilisateur-configuré était détecté et n'est pas

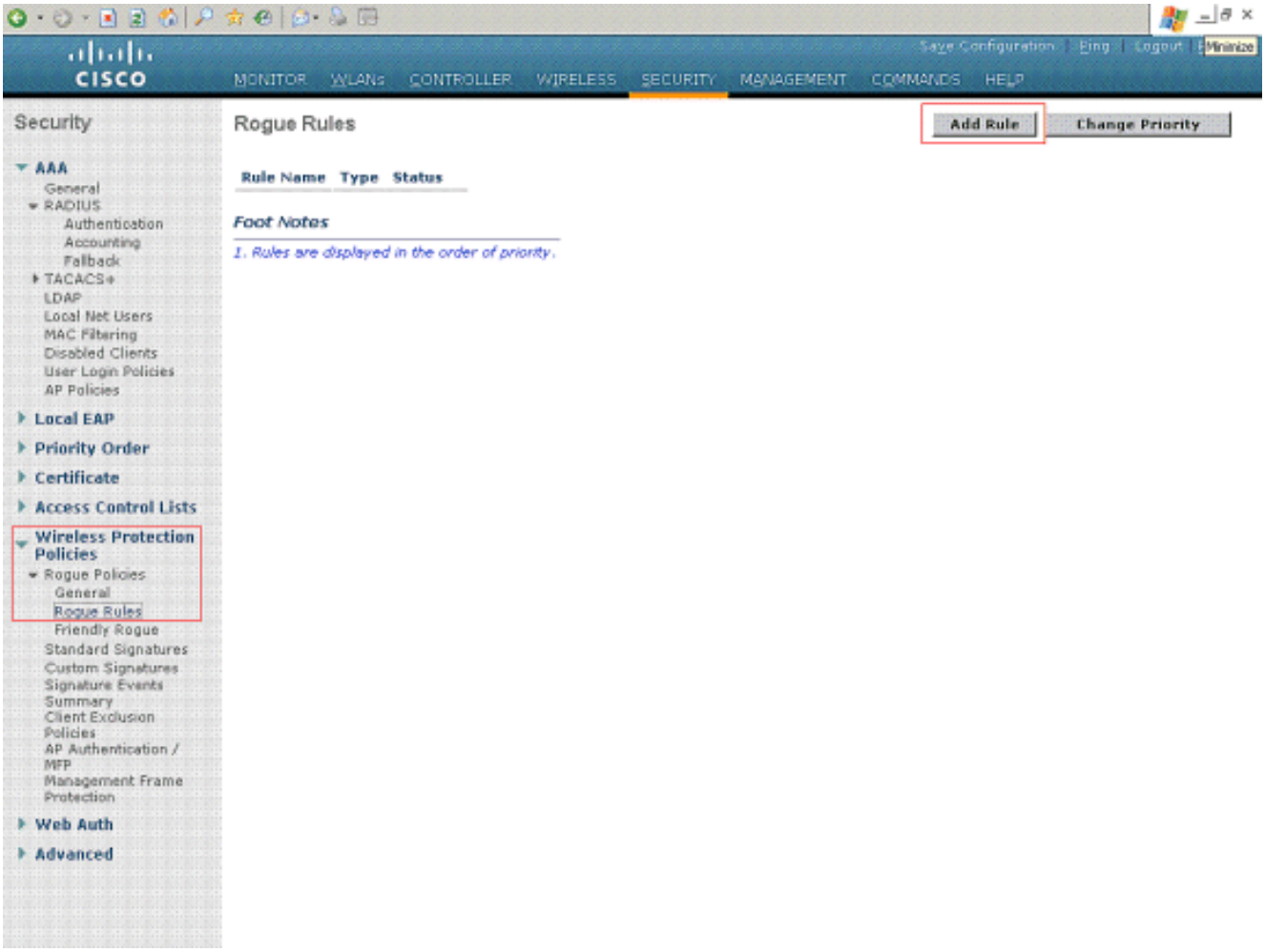
entendu pour la durée de confiance-délai d'attente, l'État voyou d'AP amical est marquée en tant que disparus de confiance.

- **Retiré —** Si AP malveillant ou non classifié n'est pas entendu de tous les contrôleurs pour la durée d'escroc-délai d'attente, l'État voyou d'AP est marquée en tant que **retiré**.

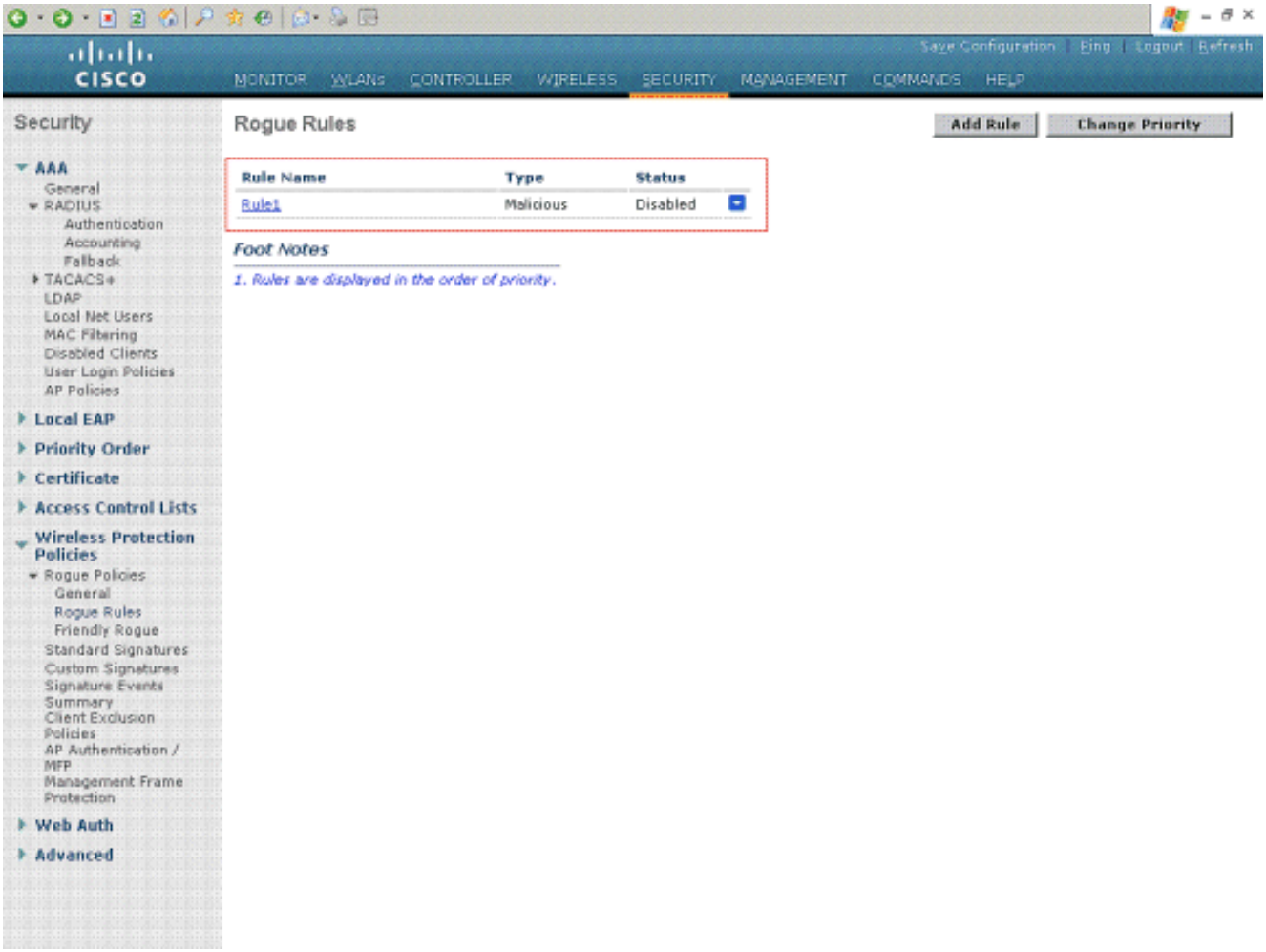
Comment configurer des règles escrocs dans WLC

Afin de configurer des règles escrocs sur le contrôleur LAN Sans fil, terminez-vous ces étapes.

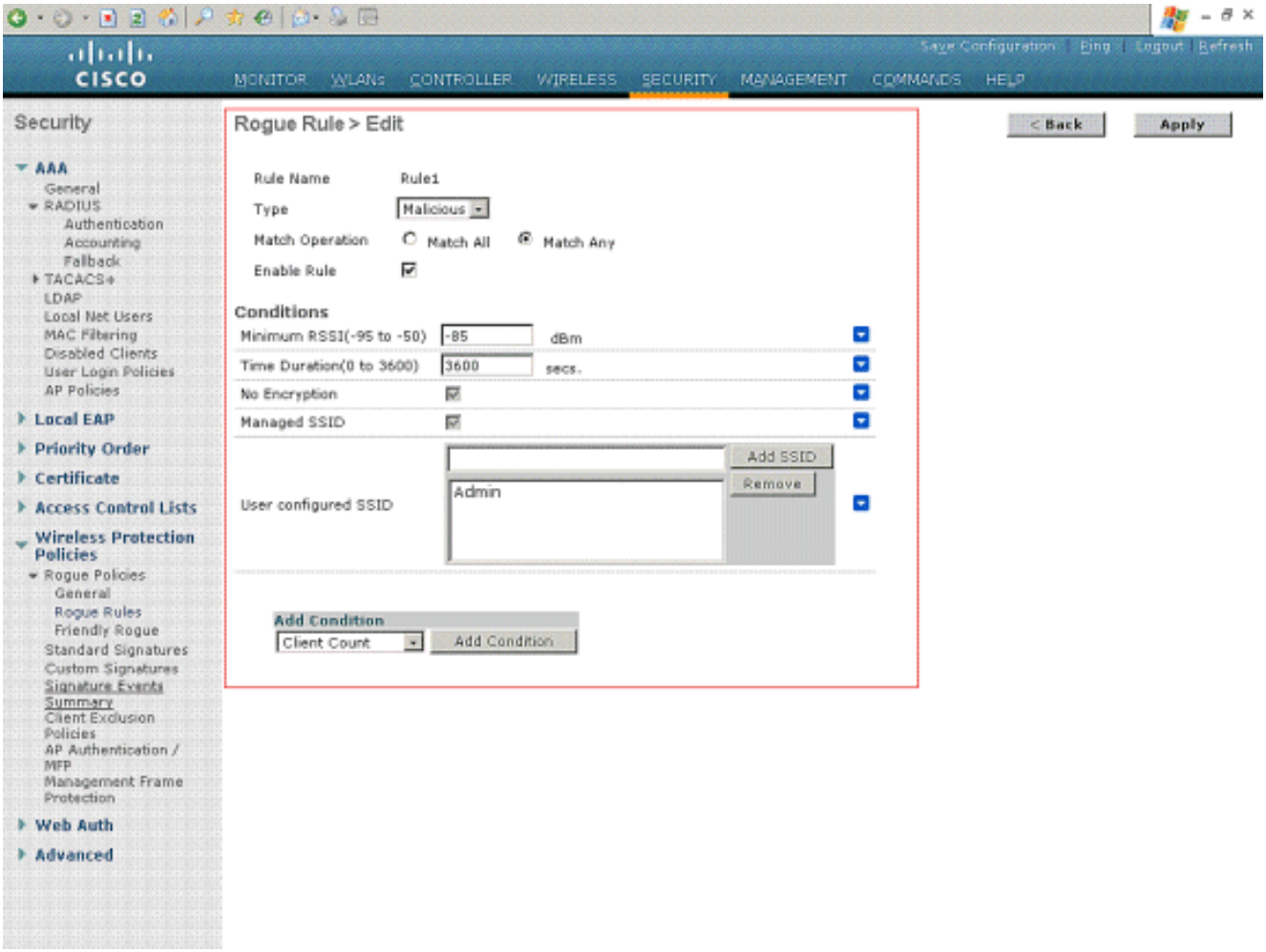
1. Des règles escrocs peuvent être créées du WLC de la page de **stratégies de Sécurité > de protection sans fil > de stratégies d'escroc > de règles d'escroc**.



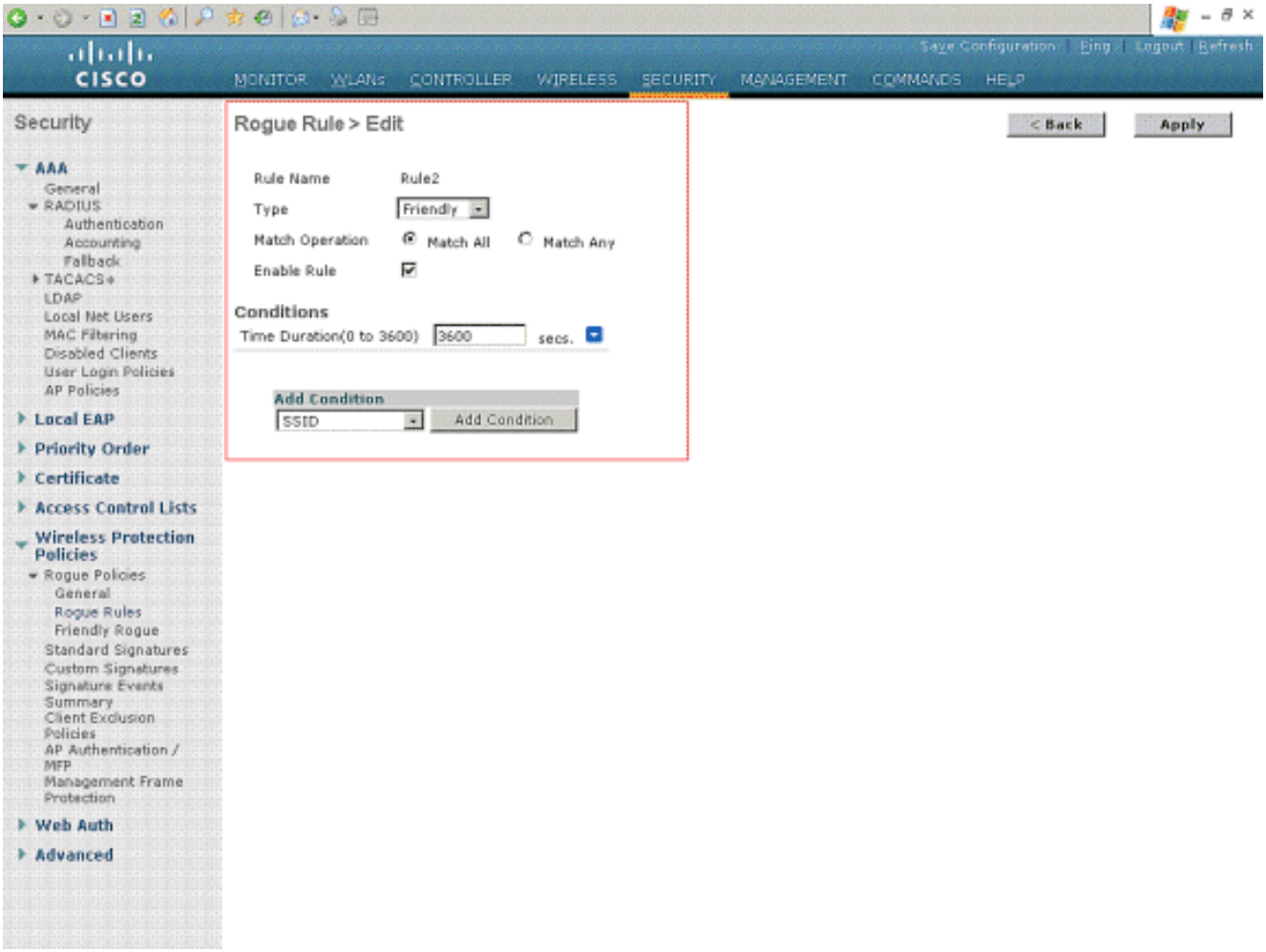
2. Afin de créer une nouvelle stratégie escroc, cliquez sur le bouton de **règle d'ajouter**. La fenêtre de **règles d'escroc** apparaît. Écrivez un nom pour la règle. Cet exemple utilise Rule1. Choisissez le type de règle. C'est un exemple d'une règle malveillante. Cliquez sur **Add**. Rule1 est créé.



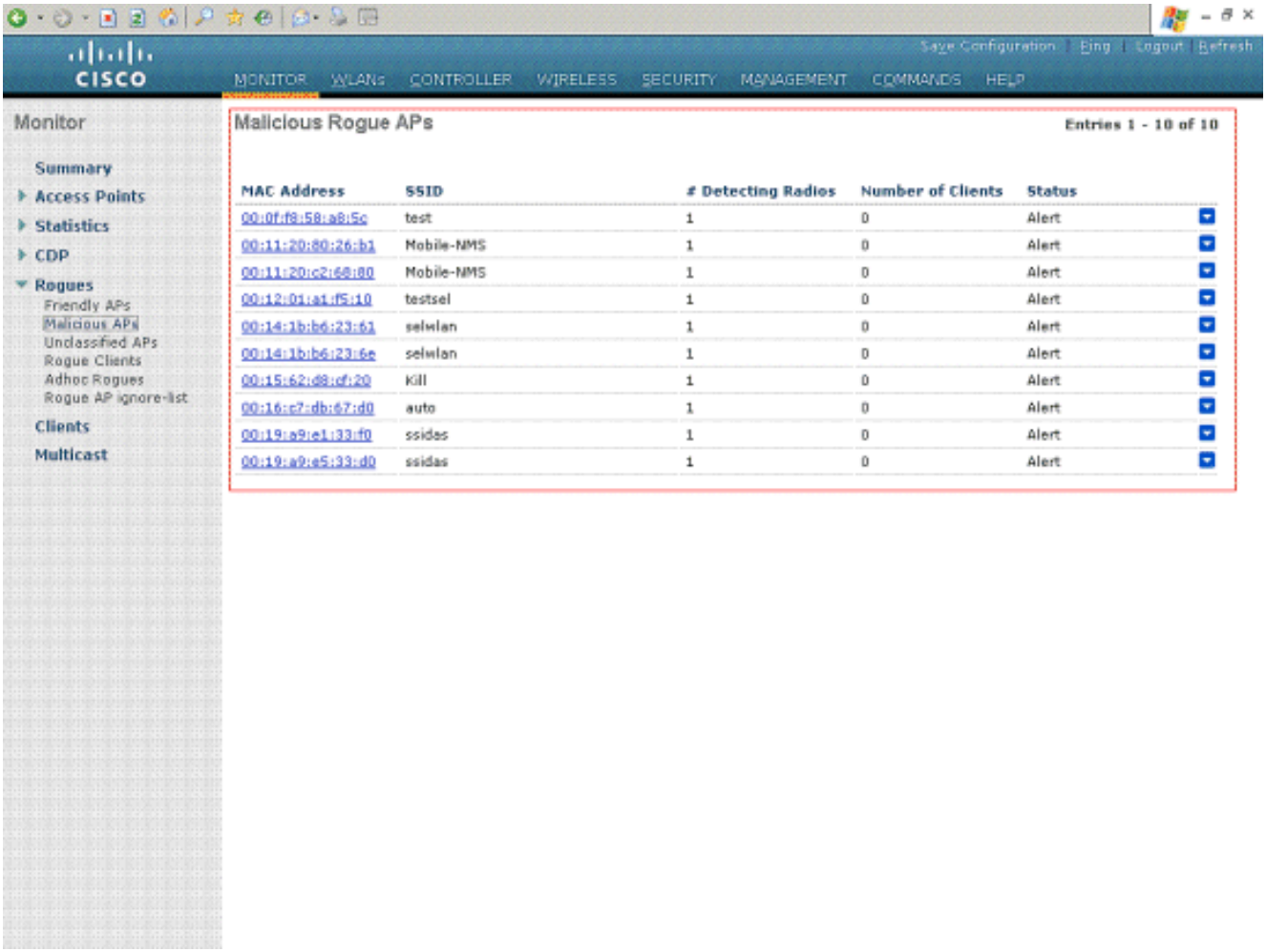
3. Afin d'éditer cette règle, cliquez sur la règle qui a été créée. **La règle escroc > éditent la** page apparaît. En cette page, cochez la case de **règle d'enable** pour lancer la règle. Choisissez le type d'exécution de correspondance et d'autres conditions basés sur le comme indiqué dans cet exemple de condition
requise.



4. C'est un exemple de la stratégie escroc amicale de règle.



5. La sortie des règles escrocs peut être vue au **moniteur > aux escrocs > AP malveillant**.

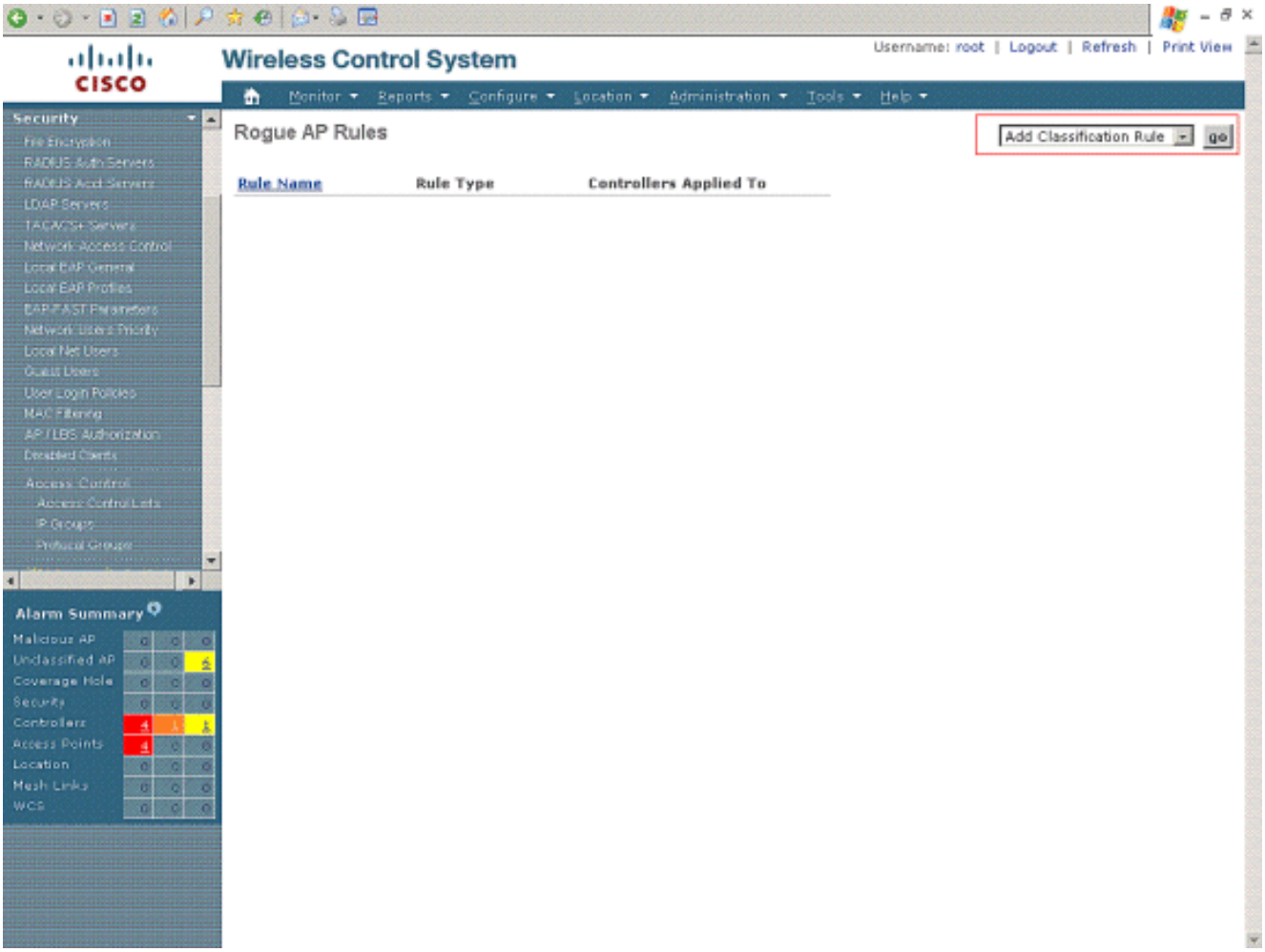


6. De même, la sortie des *règles amicales* et des *règles non classifiées* peut être visualisée au **moniteur > aux escrocs > AP non classifié** et le **moniteur > les escrocs > les** pages **amicales AP**, respectivement.

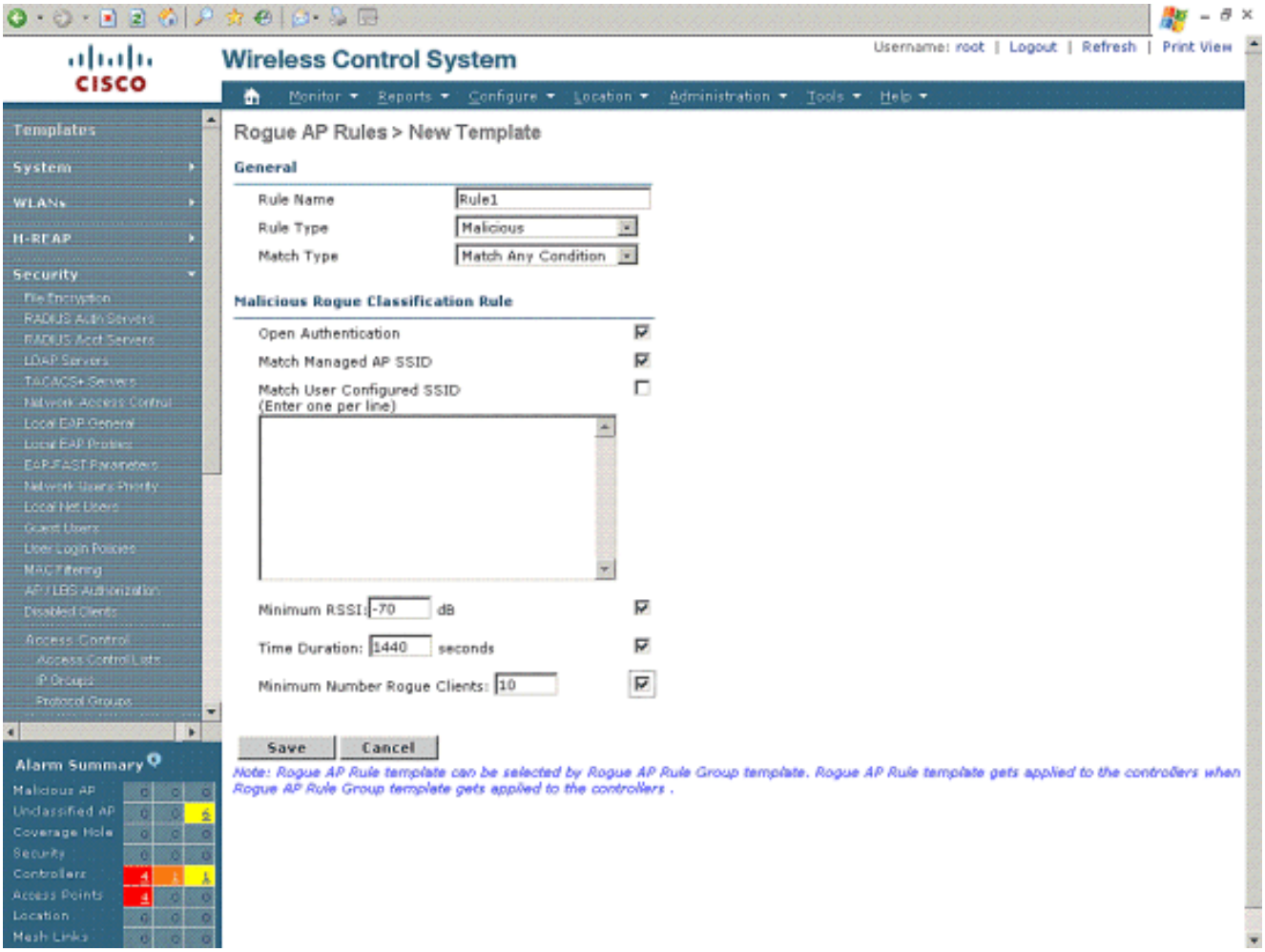
Comment configurer des règles escrocs dans WCS

Liste escroc de règle : WCS fournit l'établissement de règle d'escroc de niveau du système. Afin de configurer des règles escrocs sur WCS, terminez-vous ces étapes.

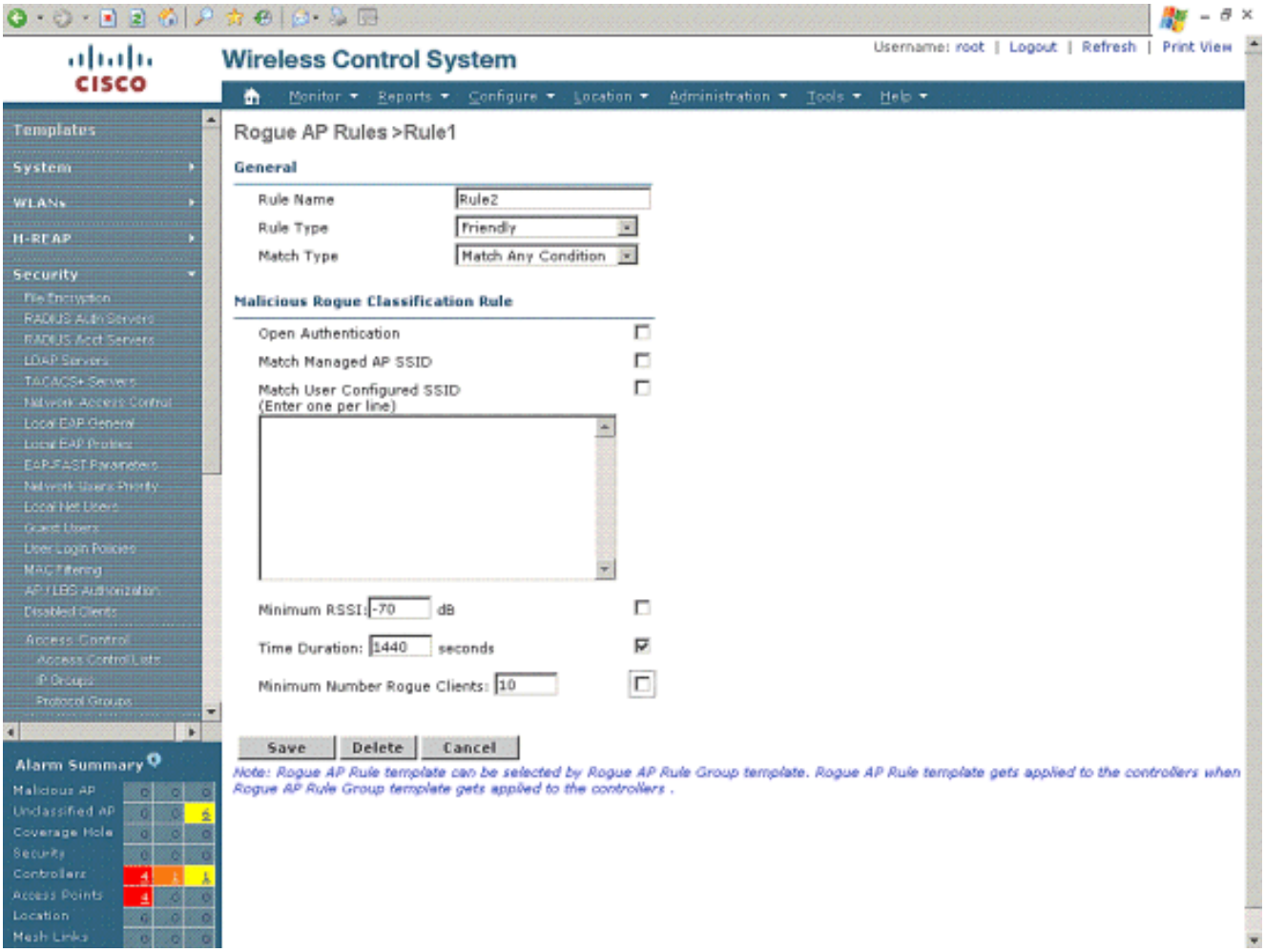
1. Choisissez **configurent > modèle de contrôleur**, et puis cliquent sur Security **> des règles de l'escroc AP** d'accéder à la page de liste de règles de l'escroc AP.
2. Cliquez sur Add la **règle de classification** sur le bon menu déroulant supérieur d'ajouter une nouvelle règle de
classification.



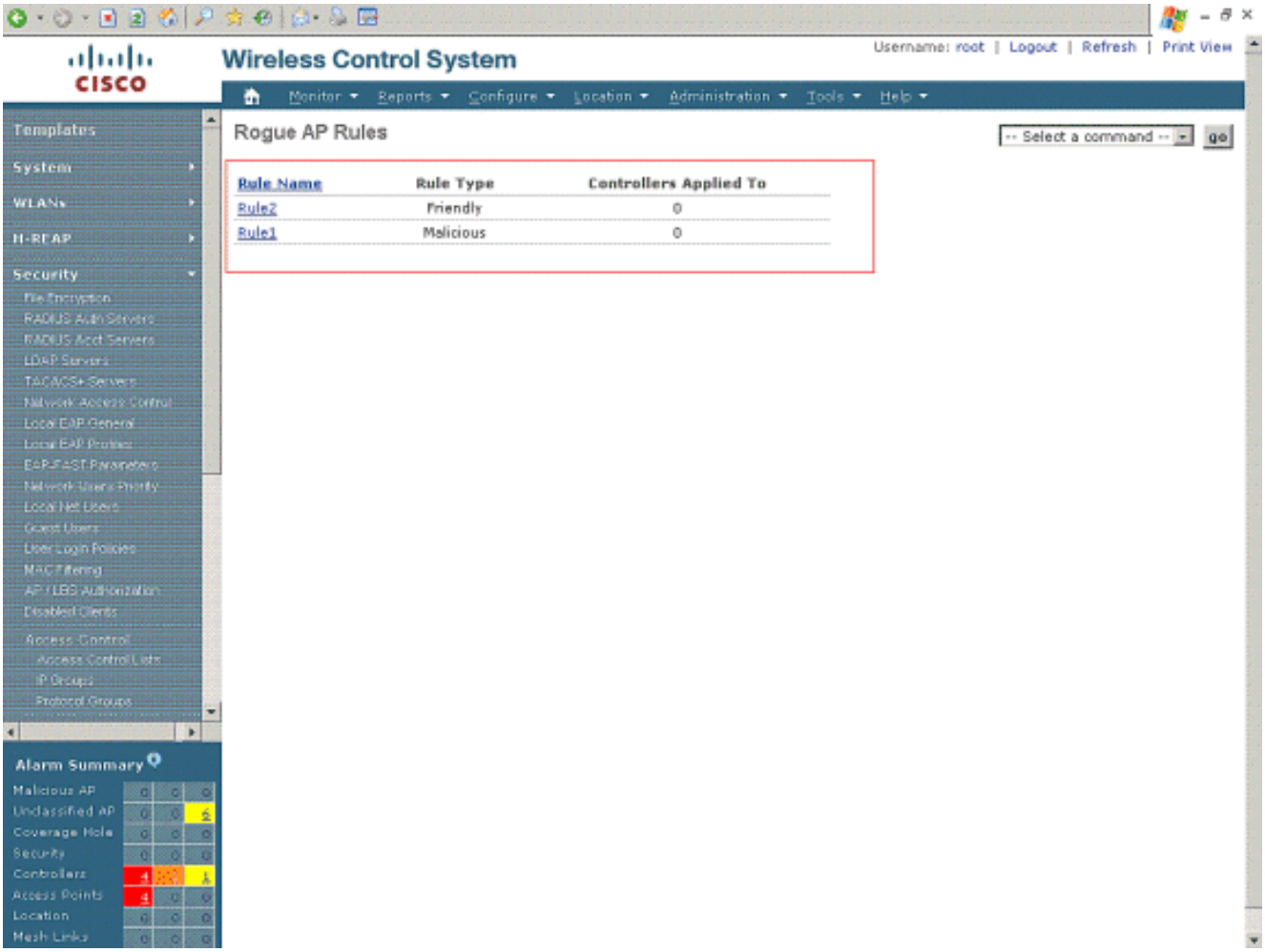
3. Cliquez sur le nom du modèle pour éditer la règle escroc. Cette page de détail de règle te permet d'éditer, de mettre à jour la règle de l'escroc AP, ou de supprimer la règle.**Règle escroc AP plaçant des paramètres :** À cette page, les utilisateurs peuvent activer n'importe quelle condition quand ils cochent la case pour concaténer le tout ou une partie de ces conditions :Aucun cryptageAP géré par correspondanceCorrespondance SSID configuré par utilisateurMinimum RSSIDuréeClient escroc de nombre minimalC'est un exemple d'une règle malveillante
:



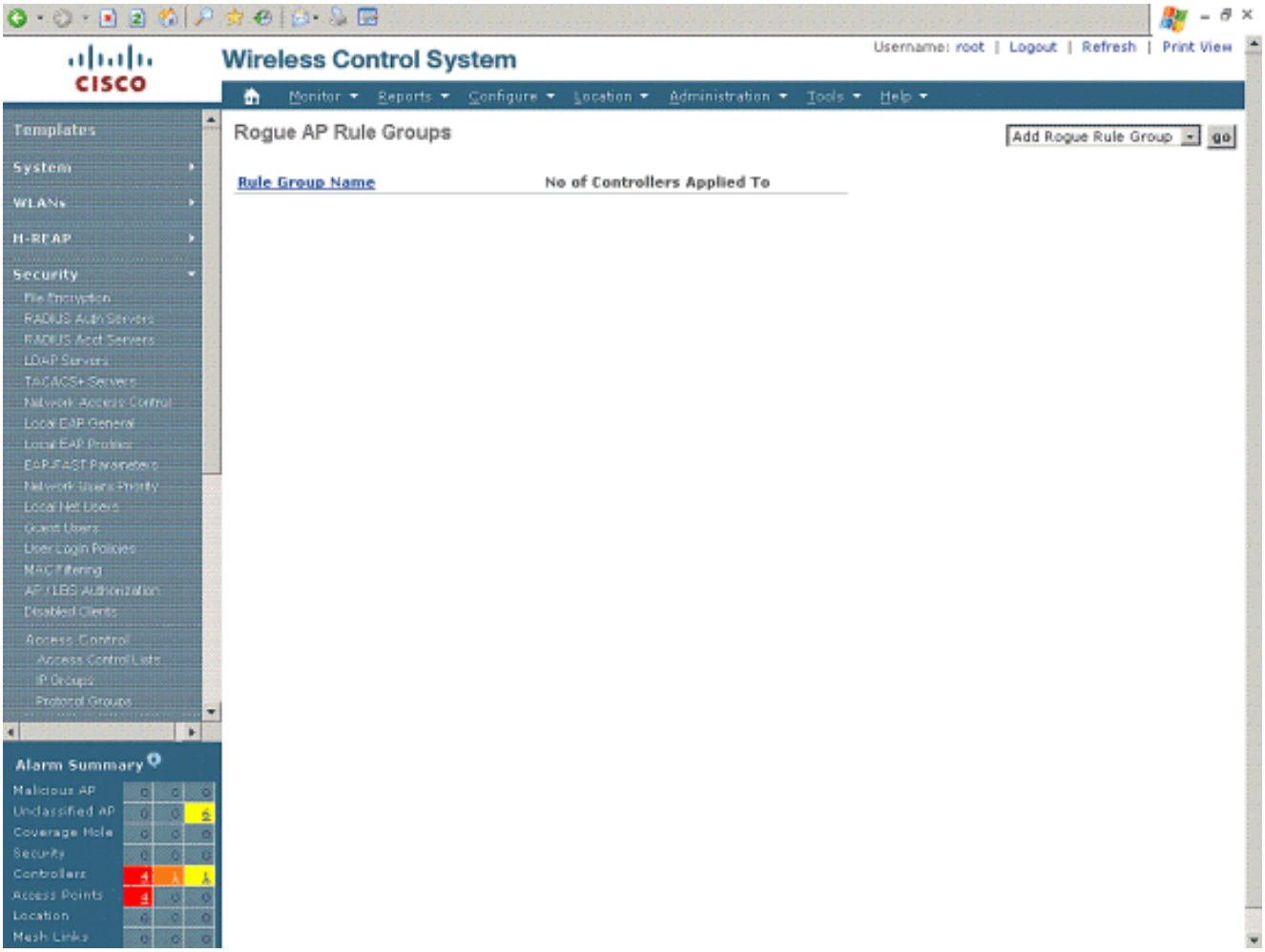
C'est un exemple d'une règle amicale
:



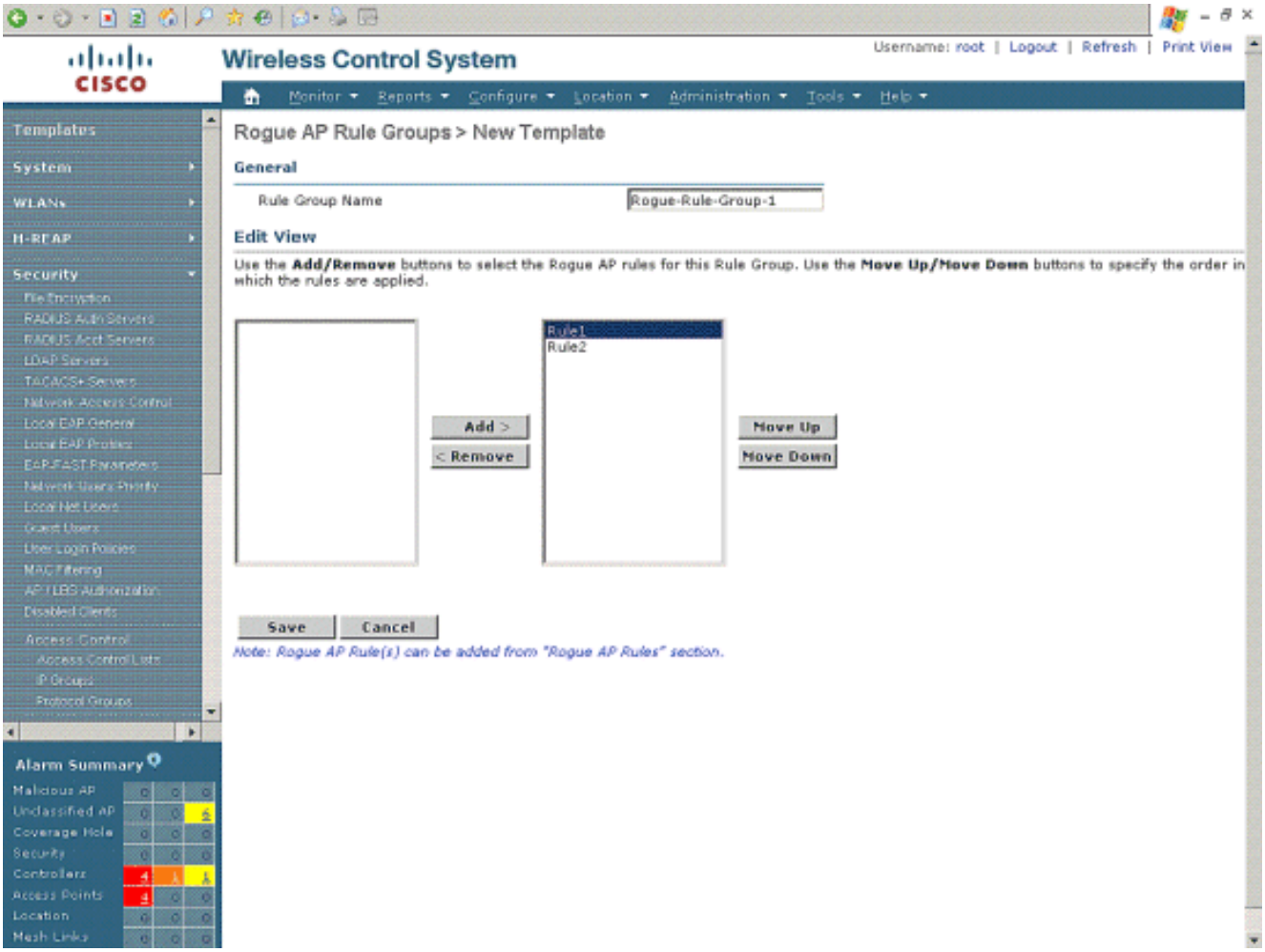
4. L'escroc qu'AP ordonne la page répertorie toutes les règles créées.



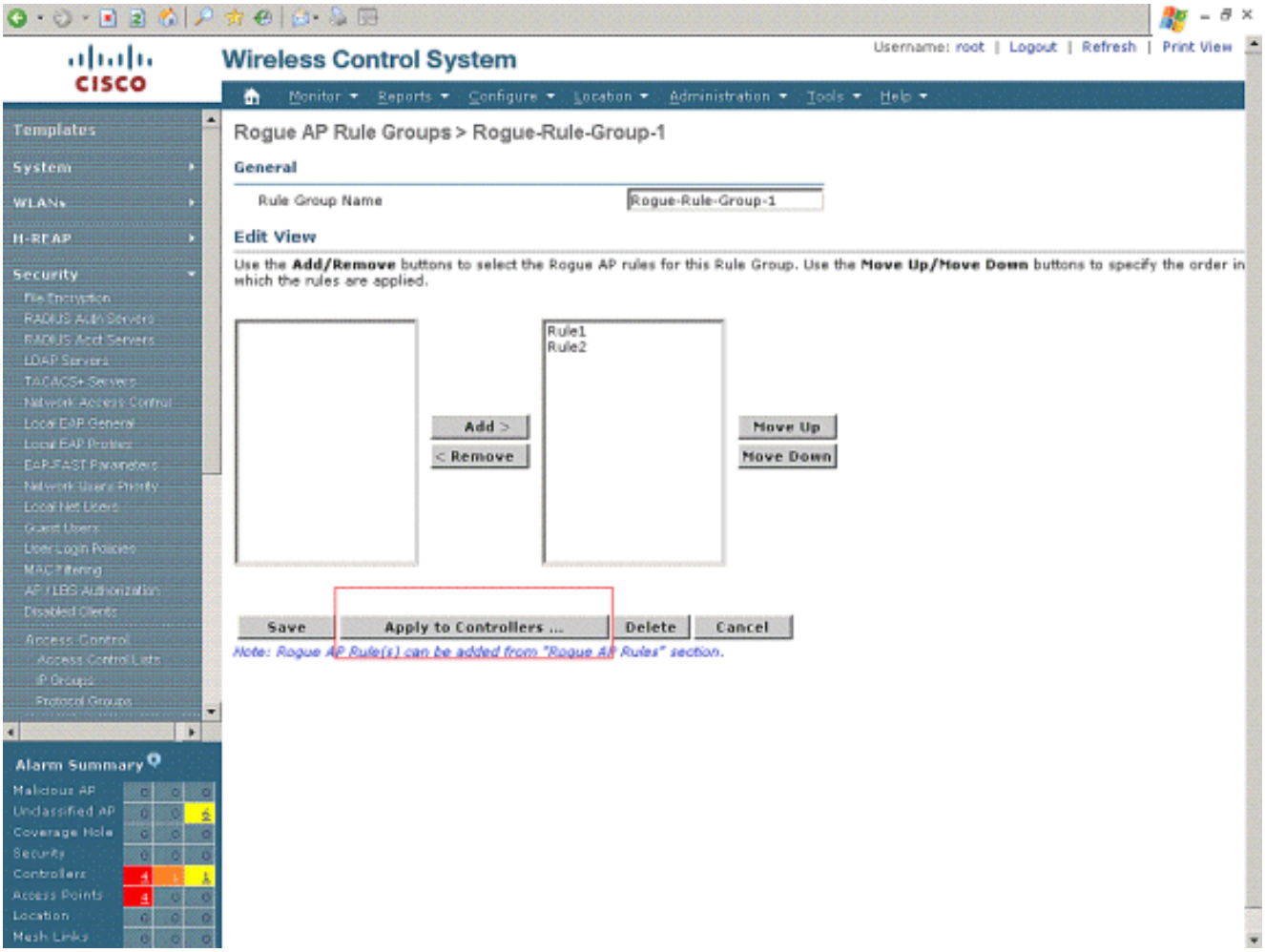
5. L'étape suivante est de configurer un groupe de règle et d'appliquer ces règles aux contrôleurs. Ceci, utilisent les **groupes de règle de l'escroc AP** plaçant sur le WCS.
6. Afin de créer un nouveau groupe de règle, choisissez **configurent > modèle de contrôleur**, et puis cliquent sur Security **> des groupes de règle de l'escroc AP du** GUI WCS.



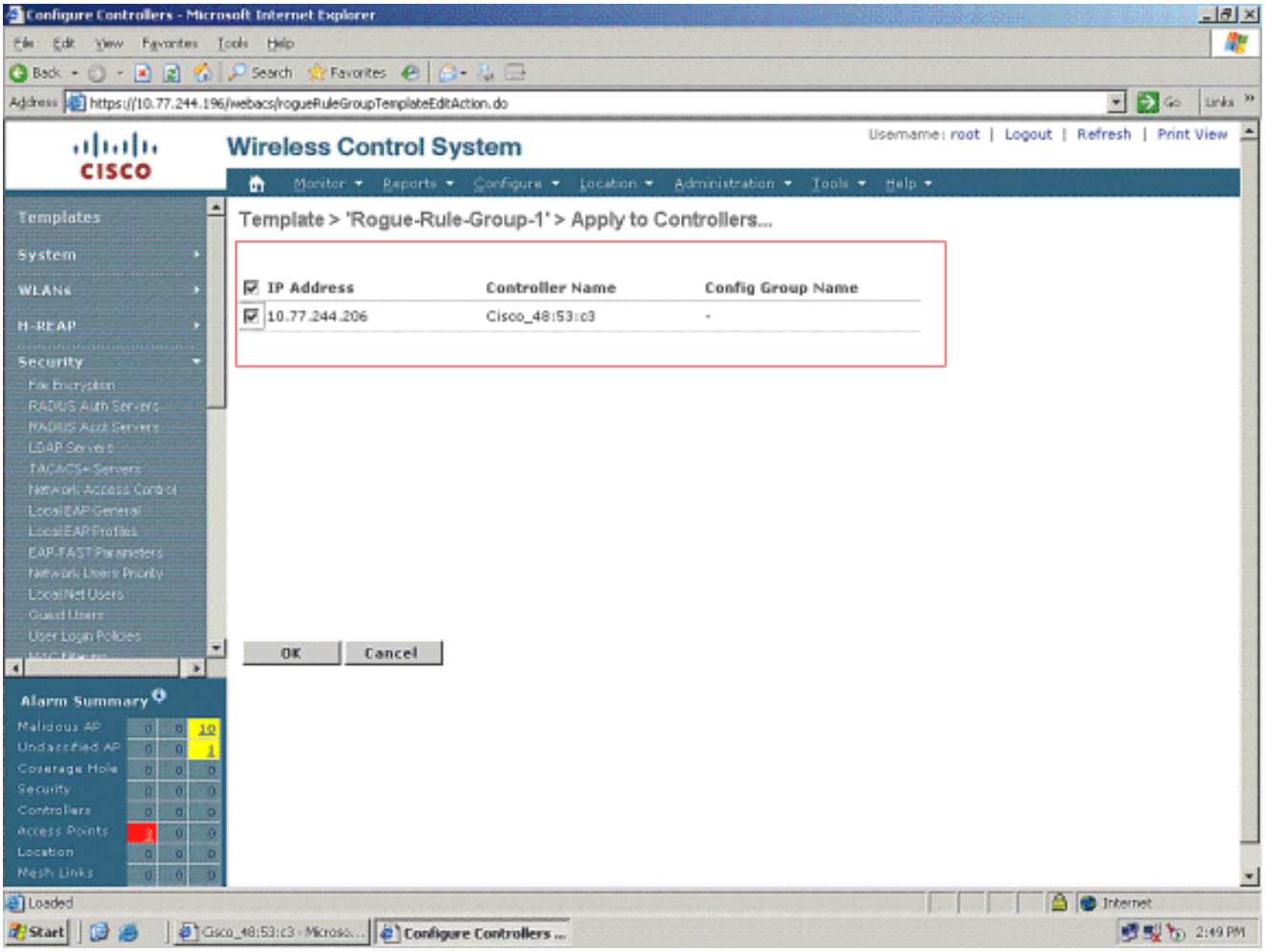
7. L'escroc que la règle AP groupe > nouvelle page de modèle te permet d'ajouter, de mettre à jour le groupe de règle de l'escroc AP, de supprimer la règle, et d'appliquer le groupe de règle au contrôleur. Utilisez les boutons d'ajout/suppression pour choisir les règles de l'escroc AP pour ce groupe de règle. Utilisez les boutons haut/bas pour spécifier la commande dans laquelle les règles sont appliquées. Voici un exemple : Une fois que le groupe de règles est configuré, **sauvegarde de**
clic.



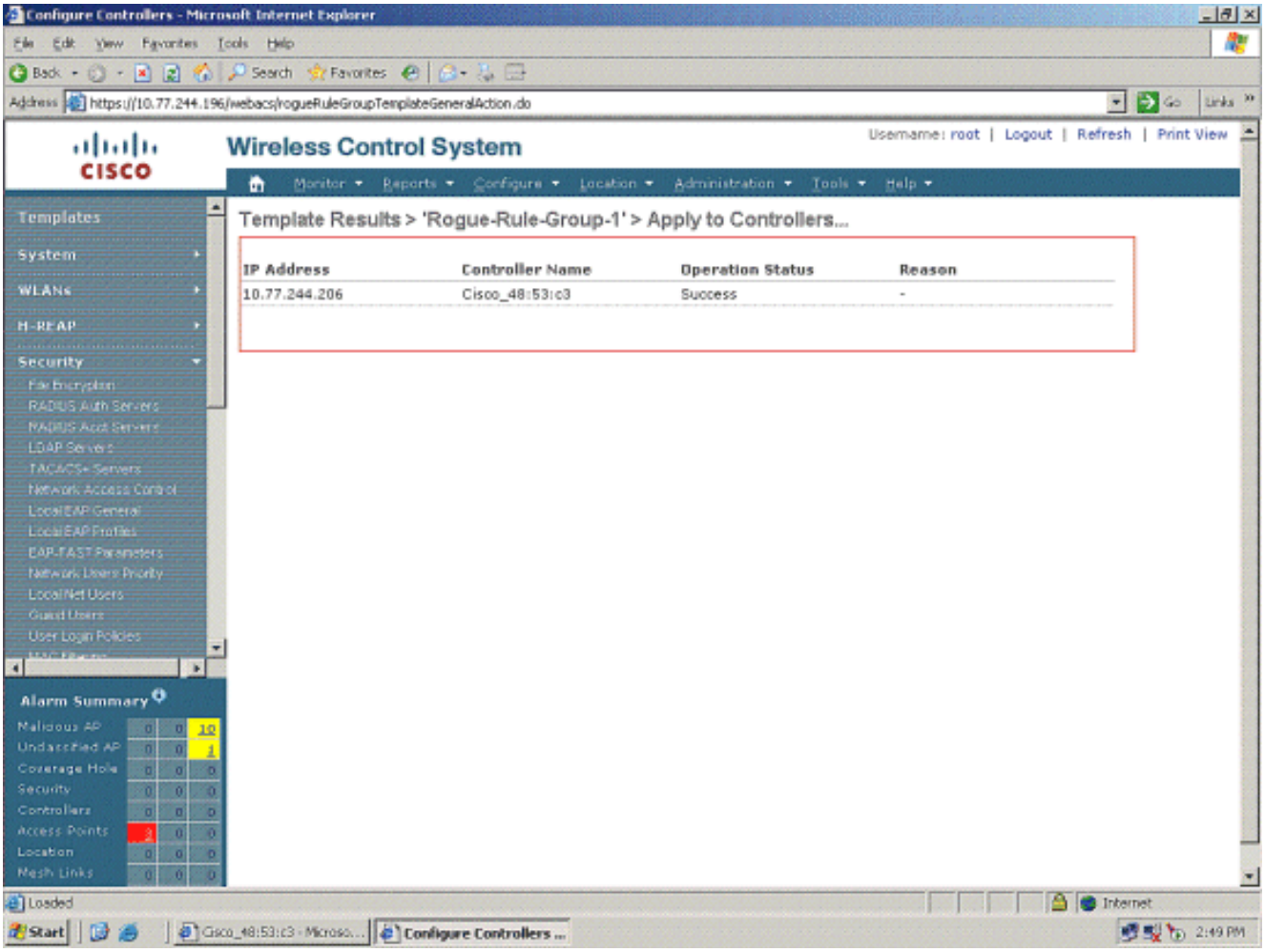
8. Une fois que vous épargnez le groupe de règle, il peut être appliqué aux contrôleurs. Afin d'appliquer le groupe de règle au contrôleur, éditez le groupe de règle. Cliquez sur le nom de groupe de
règle.



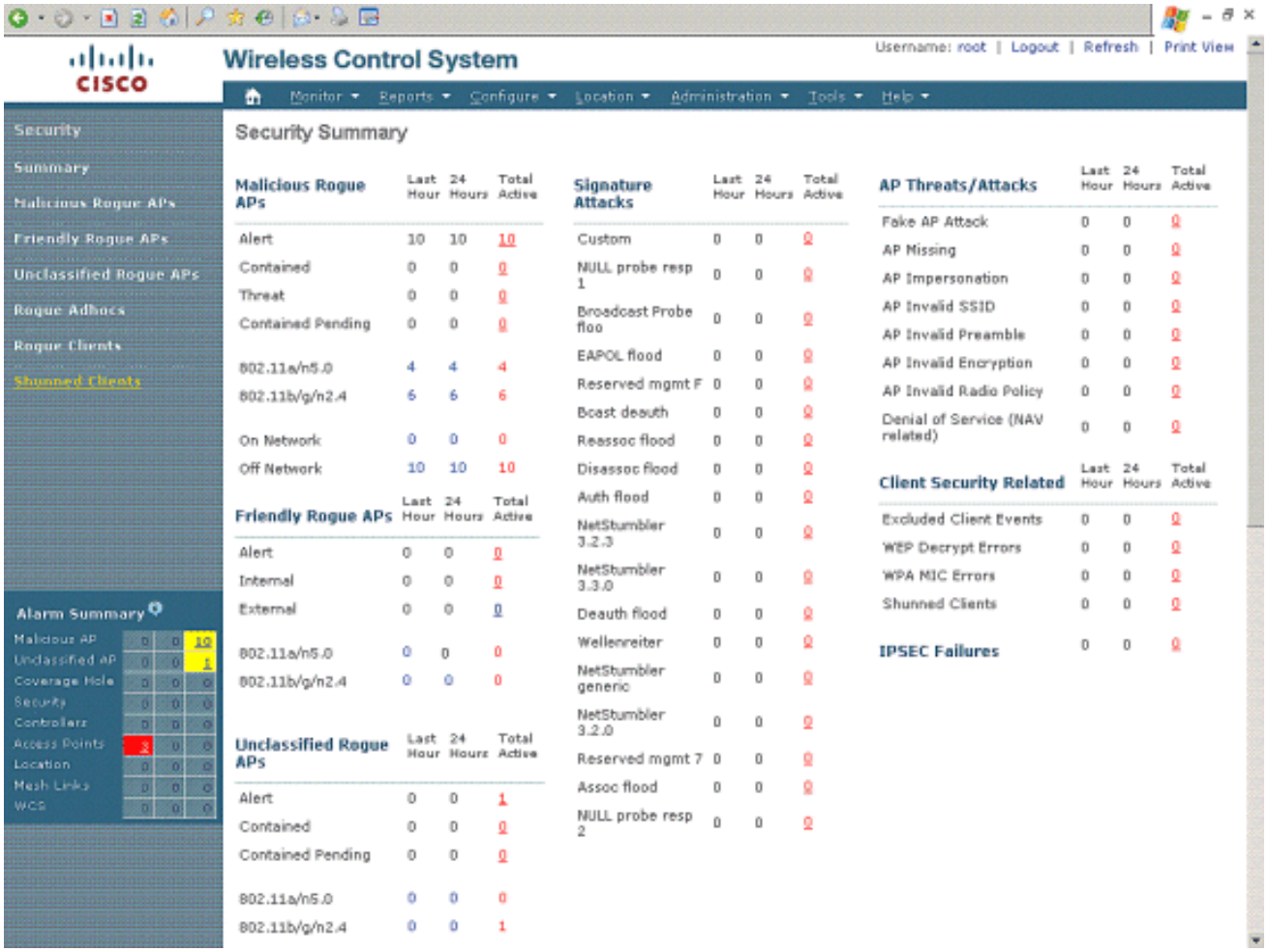
Cliquez sur Apply aux **contrôleurs**. Sur la page suivante, choisissez les contrôleurs auxquels cette règle est appliquée. Voici un exemple
:



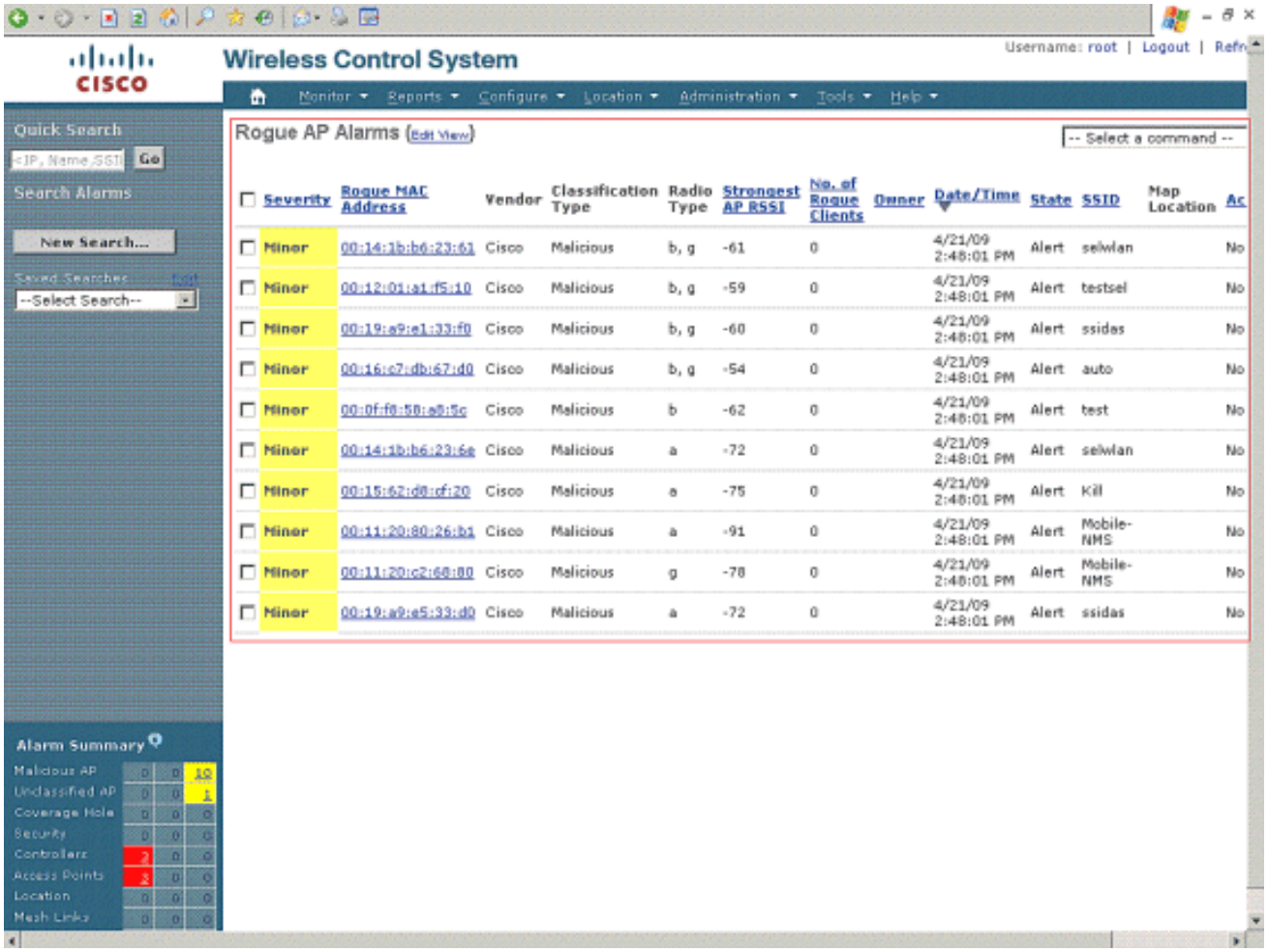
9. Une fois que les règles sont appliquées aux contrôleurs, vous voyez un message de **succès** sur le
WCS.



10. Des détails au sujet des aps classifiés peuvent être visualisés à la page **récapitulative de Sécurité**. Voici un exemple
    :



11. Des détails au sujet des aps classifiés, des aps spécifiquement malveillants, amicaux, et non classifiés, peuvent être visualisés quand vous cliquez sur la classification appropriée de la page récapitulative de Sécurité. C'est un exemple pour les aps malveillants.



Informations connexes

- Détection de systèmes indésirables sous des réseaux sans fil unifiés
- Support et documentation techniques - Cisco Systems