Filtres d'ACL sur l'exemple de configuration de l'Aironet aps

Contenu

Introduction

Ce document décrit comment configurer les filtres basés sur de liste de contrôle d'accès (ACL) sur les Points d'accès de Cisco Aironet (aps) avec l'utilisation du GUI.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration d'une connexion sans fil à l'aide d'un AP Aironet et d'un adaptateur client Aironet 802.11 a/b/g
- ACLs

[Composants utilisés](#)

Ce document utilise la gamme 1040 aps d'Aironet qui exécutent la version de logiciel 15.2(2)JB de Cisco IOS®.

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.

Informations générales

Vous pouvez utiliser des filtres sur des aps afin d'effectuer ces tâches :

- Restreindre l'accès au réseau sans fil LAN (WLAN)
- Fournir une couche supplémentaire de sécurité sans fil

Vous pouvez employer différents types de filtres afin de filtrer le trafic basé en fonction :

- de protocoles spécifiques ;
- L'adresse MAC du périphérique de client
- L'adresse IP du périphérique de client

Vous pouvez également permettre à des filtres afin de limiter le trafic des utilisateurs sur le lan câblée. Les filtres d'adresse IP et d'adresse MAC permettent ou rejettent le transfert des paquets de monodiffusion et de multidiffusion qui sont envoyés vers ou depuis des adresses IP ou MAC spécifiques.

Les filtres basés sur des protocoles fournissent une façon plus précise de restreindre l'accès aux protocoles spécifiques par les interfaces Ethernet et radios de l'AP. Vous pouvez employer l'un ou l'autre de ces méthodes afin de configurer les filtres sur les aps :

- GUI Web
- CLI

Ce document explique comment employer ACLs afin de configurer des filtres par le GUI.

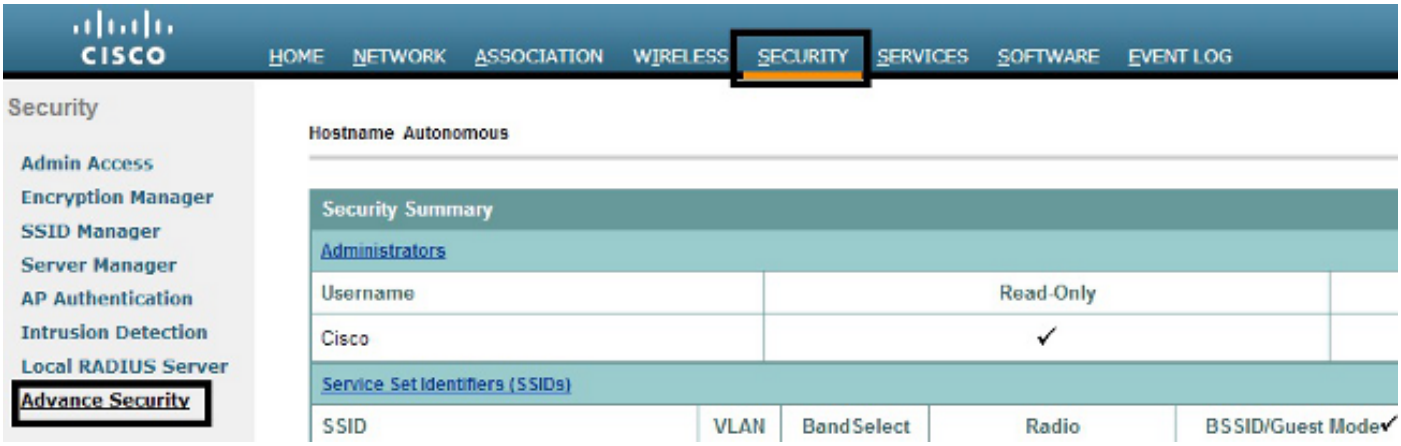
> Remarque: Pour plus d'informations sur la configuration par l'utilisation du CLI, référez-vous à l'article de Cisco d'exemple de configuration de filtre d'ACL de Point d'accès.

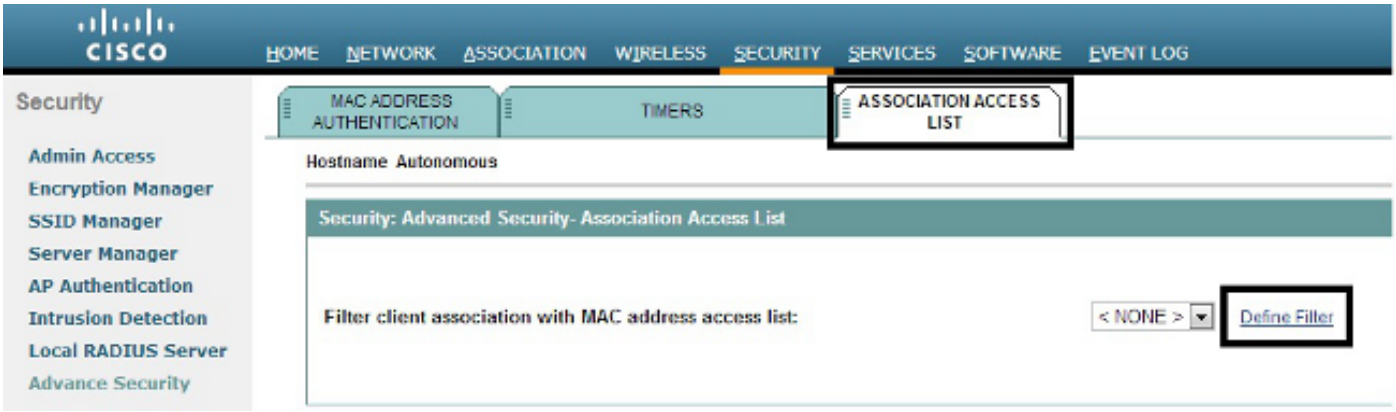
Configurez

Cette section décrit comment configurer les filtres basés sur acl sur Cisco Aironet aps avec l'utilisation du GUI.

Où créer ACLs

Naviguez vers la **Sécurité** > la **Sécurité à l'avance**. Choisissez l'onglet de **liste d'accès d'association**, et le clic **définissent le filtre** :



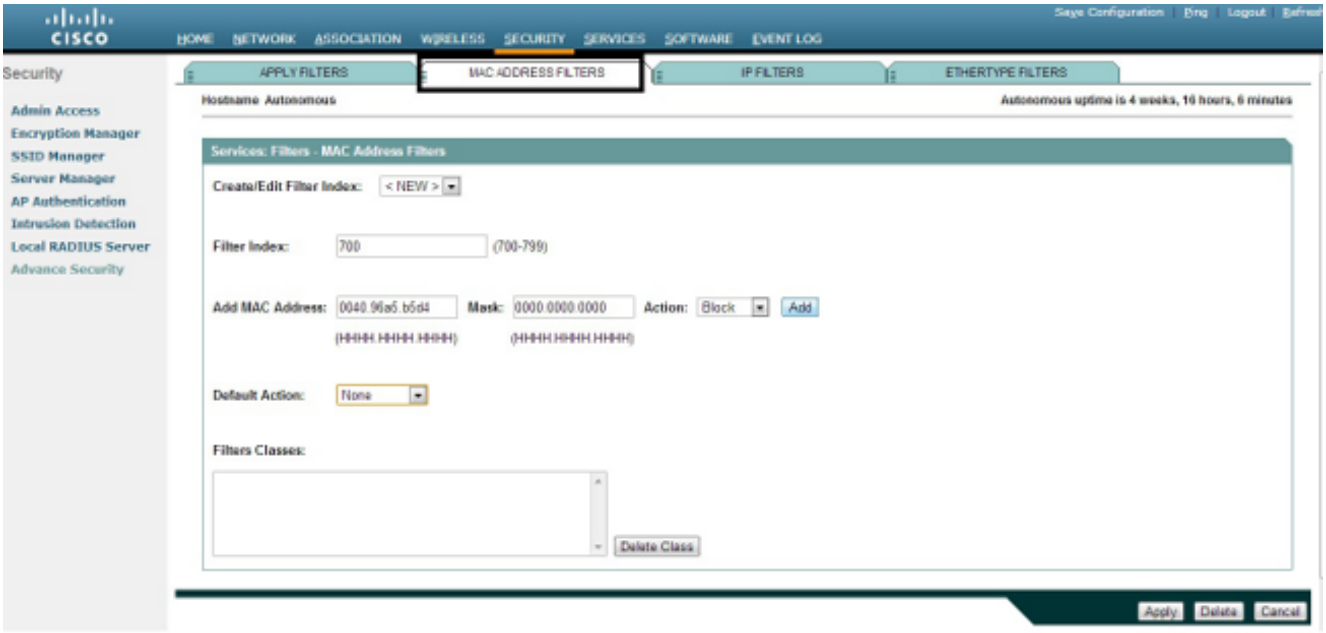


Filtres d'adresse MAC

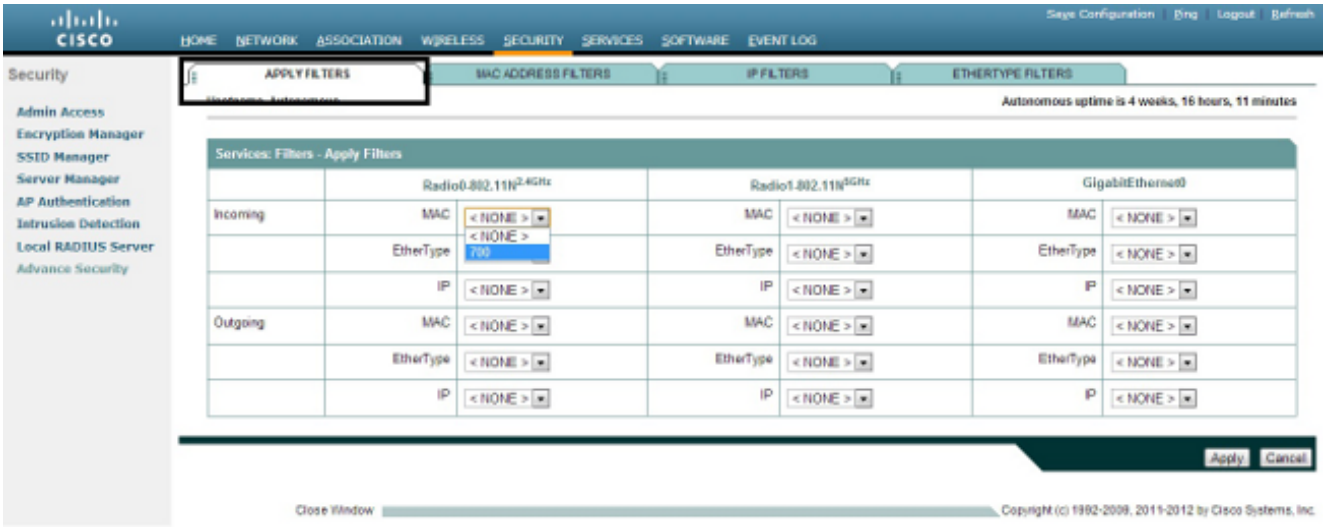
Vous pouvez utiliser les filtres basés sur adresse de MAC afin de filtrer des périphériques de client basés sur l'adresse MAC dur-codée. Quand un client se voit refuser l'accès par un filtre basé sur l'adresse MAC, il ne peut pas s'associer à l'AP. Les filtres d'adresse MAC permettent ou rejettent l'expédition de l'unicast et des paquets de multidiffusion envoyés, ou adressés, derrière les adresses MAC spécifiques.

Cet exemple montre comment configurer un filtre basé sur MAC par le GUI afin de filtrer le client avec une adresse MAC de **0040.96a5.b5d4** :

1. Créez l'**ACL 700 d'**adresse MAC. Cette ACL ne permet pas au client 0040.96a5.b5d4 de s'associer à l'AP.



2. Cliquez sur Add afin d'ajouter ce filtre aux classes de filtres. Vous pouvez également définir l'action par défaut en tant qu'**en avant tout** ou **refuser tous**.
3. Cliquez sur **Apply**. **L'ACL 700** est maintenant créé.
4. Afin de s'appliquer l'**ACL 700 à une** interface par radio, naviguez vers la section de **filtres d'application**. Vous pouvez maintenant s'appliquer cet ACL à un entrant ou la radio ou les GigabitEthernets sortants relient.



Filtres IP

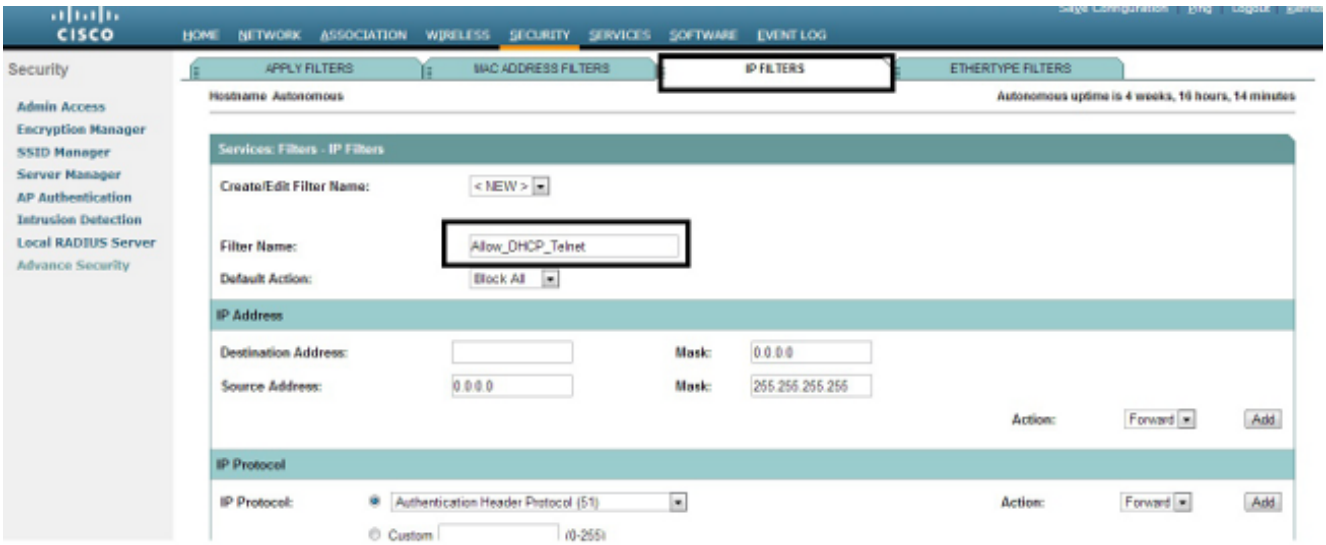
Vous pouvez utiliser ACLs standard ou étendu afin de permettre ou rejeter l'entrée des périphériques de client dans le réseau WLAN basé sur l'adresse IP du client.

Utilisations ACLs étendu de cet exemple de configuration. L'ACL étendu doit permettre l'accès de telnet aux clients. Vous devez restreindre tous les autres protocoles sur le réseau WLAN. En outre, les clients emploient le DHCP afin d'obtenir l'adresse IP. Vous devez créer une liste de contrôle d'accès étendue qui :

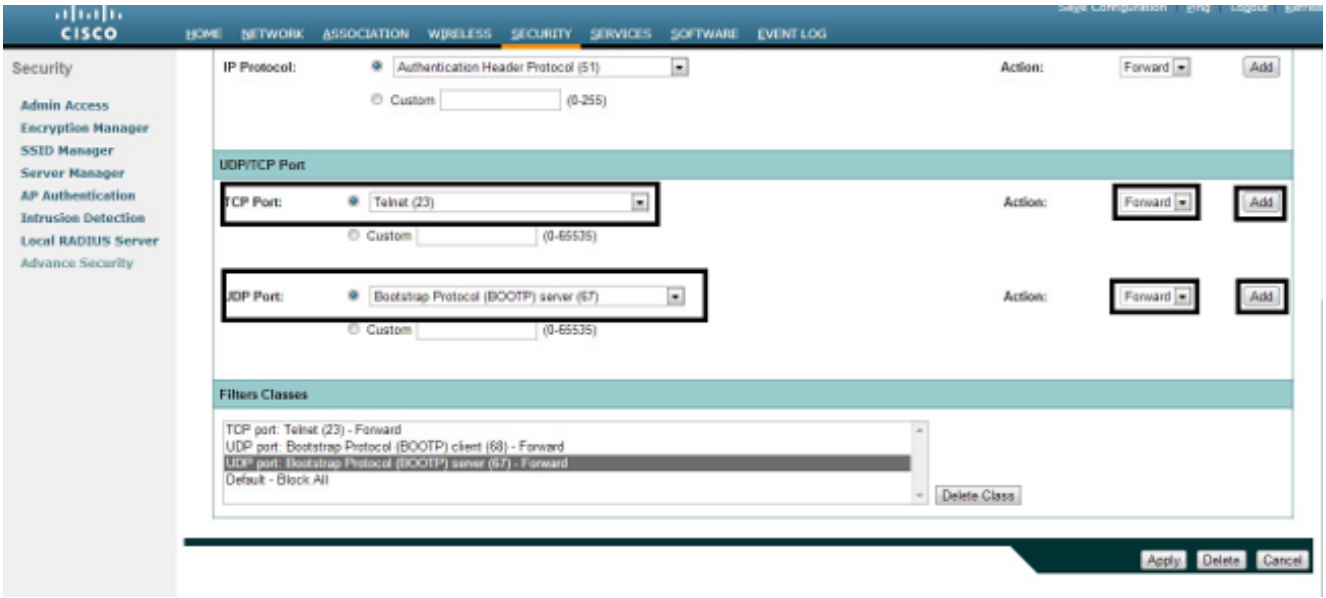
- permet le trafic DHCP et Telnet ;
- refuse tous les autres types de trafic.

Terminez-vous ces étapes afin de le créer :

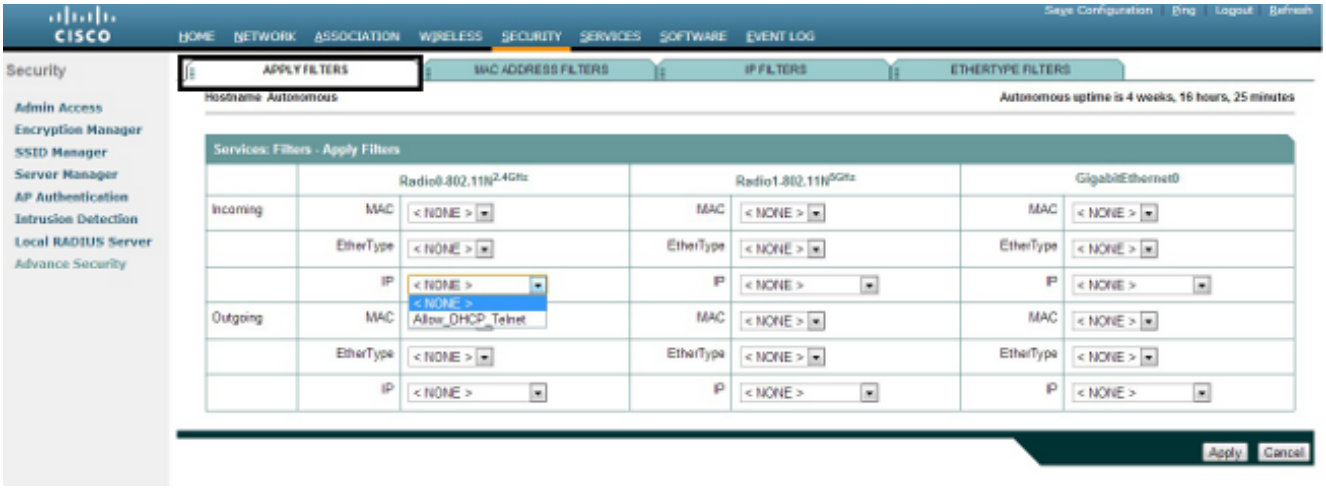
1. Nommez le filtre, et sélectionnez le **bloc tout de la** liste déroulante d'**action par défaut**, puisque le trafic restant doit être bloqué :



2. **Telnet** choisi de la liste déroulante de **port TCP**, et **client de Protocole BOOTP** et **serveur de Protocole BOOTP de la** liste déroulante de **port UDP** :



3. Cliquez sur **Apply**. Le filtre IP **Allow_DHCP ? le _Telnet** est maintenant créé, et vous pouvez s'appliquer cet ACL à un entrant ou la radio ou les GigabitEthernets sortants relient.

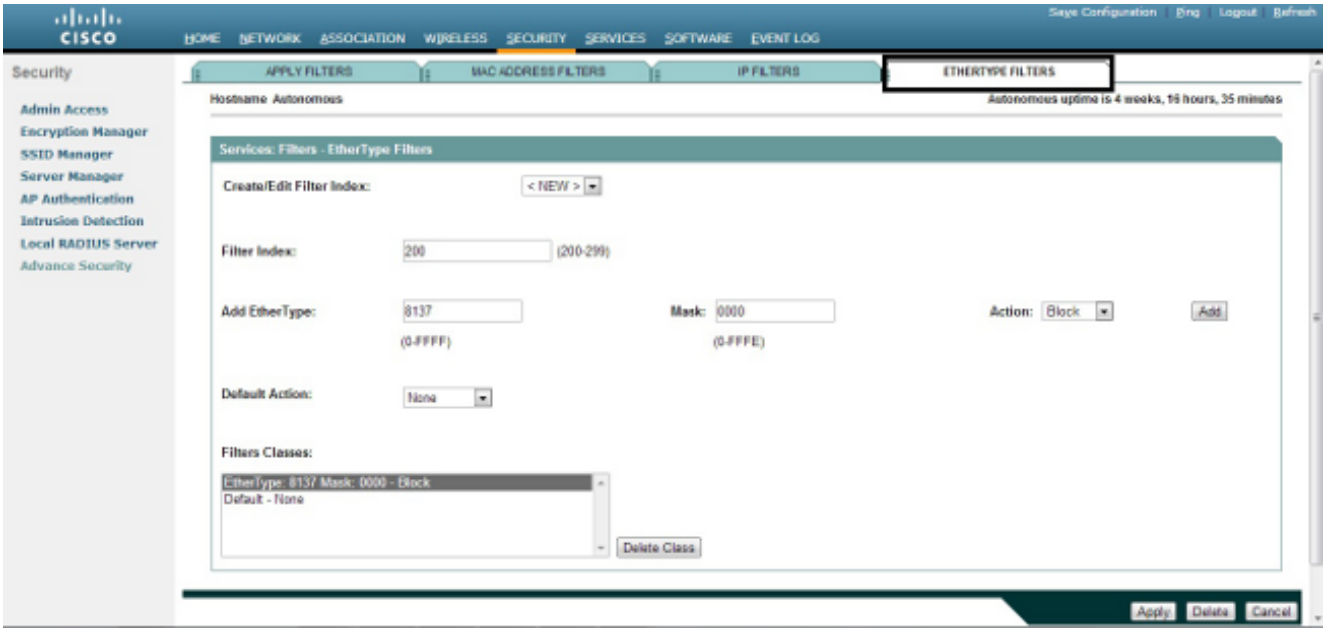


Filtres d'Ethertype

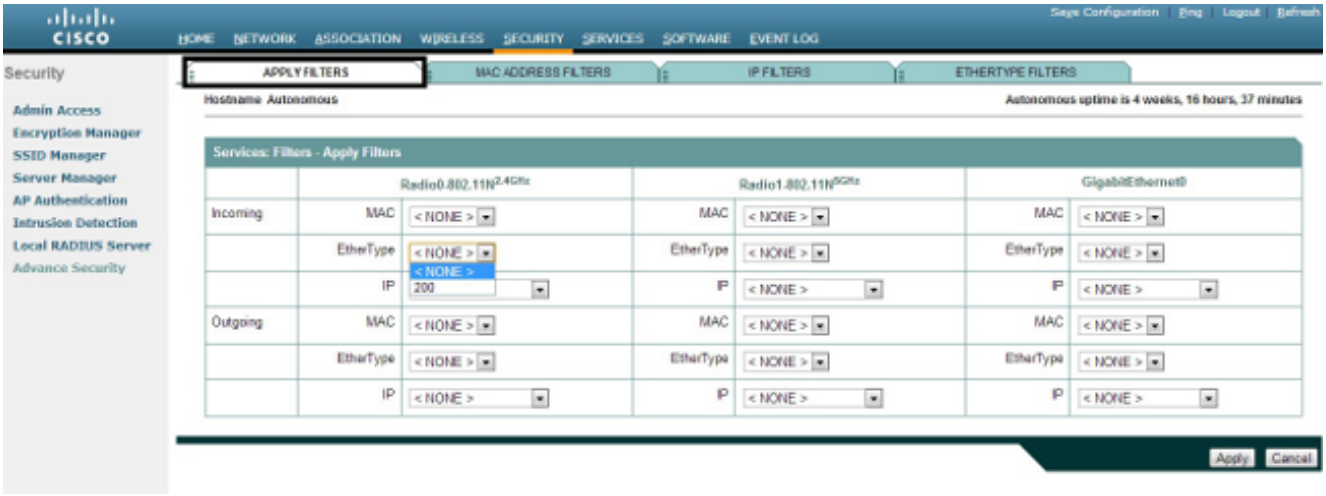
Vous pouvez utiliser des filtres d'Ethertype afin de bloquer le trafic de l'Internetwork Packet Exchange (IPX) sur Cisco Aironet AP. Une situation typique où c'est utile est quand les émissions de serveur IPX obstruent la liaison sans fil, qui se produit parfois sur un grand réseau d'entreprise.

Terminez-vous ces étapes afin de configurer et appliquer un filtre qui bloque le trafic IPX :

1. Cliquez sur l'onglet de **filtres d'Ethertype**.
2. Dans le domaine d'**index de filtre**, nommez le filtre avec un nombre de 200 à 299. Le nombre que vous assignez crée un ACL pour le filtre.
3. Écrivez **8137** dans le domaine d'**Ethertype d'ajouter**.
4. Laissez le masque pour l'Ethertype dans le **masque pour mettre en place à la** valeur par défaut.
5. Sélectionnez le **bloc du** menu d'action, et cliquez sur Add.



6. Afin de retirer l'Ethertype de la liste de classes de filtres, le sélectionner, et cliquer sur Delete la **classe**. Répétez les étapes précédentes, et ajoutez les types **8138**, **00ff**, et **00e0 au** filtre. Vous pouvez maintenant s'appliquer cet ACL à un entrant ou la radio ou les GigabitEthernets sortants relient.


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENT LOG
Security
Admin Access
Encryption Manager
SSID Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security
APPLY FILTERS
MAC ADDRESS FILTERS
IP FILTERS
ETHERTYPE FILTERS
Hostname Autonomous
Autonomous uptime is 4 weeks, 16 hours, 37 minutes
Services: Filters - Apply Filters
Radio0-802.11N2.4GHz
Radio1-802.11N5GHz
GigabitEthernet0
Incoming
Outgoing
MAC
EtherType
IP
< NONE >
200
Apply
Cancel