Aironet AP での ACL フィルタの設定例

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[ACL の作成場所](#)
[MAC アドレス フィルタ](#)
[IP フィルタ](#)
[Ethertype フィルタ](#)

概要

このドキュメントでは、GUI を使用して Cisco Aironet アクセス ポイント（AP）上でアクセス コントロール リスト（ACL）ベースのフィルタを設定する方法について説明します。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Aironet AP および Aironet 802.11 a/b/g クライアント アダプタを使用する無線接続の設定。
- ACL

使用するコンポーネント

このドキュメントは、Cisco IOS® ソフトウェア リリース 15.2(2)JB が動作する Aironet 1040 シリーズ AP を使用します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

AP でフィルタを使用すると、次の作業を実行できます。

- 無線 LAN（WLAN）ネットワークへのアクセス制限。
- 無線セキュリティのレイヤの追加。

以下の項目に基づいたトラフィックのフィルタリングには、さまざまなタイプのフィルタを使用できます。

- 特定のプロトコル
- クライアント デバイスの MAC アドレス
- クライアント デバイスの IP アドレス

また、フィルタを有効にして、有線 LAN 上のユーザからのトラフィックを制限することもできます。 IP アドレスと MAC アドレスのフィルタによって、特定の IP アドレスや MAC アドレス間で送受信されるユニキャストおよびマルチキャスト パケットの転送を許可または禁止できます。

プロトコル ベースのフィルタでは、さらに詳細なフィルタを行うことができ、AP のイーサネット インターフェイスと無線インターフェイスを通過する特定のプロトコルへのアクセスを制限できます。 AP 上でのフィルタの設定には、以下のいずれかの方法を使用できます。

- Web GUI
- CLI

このドキュメントでは、GUI でフィルタを設定するための、ACL の使用方法について説明します。

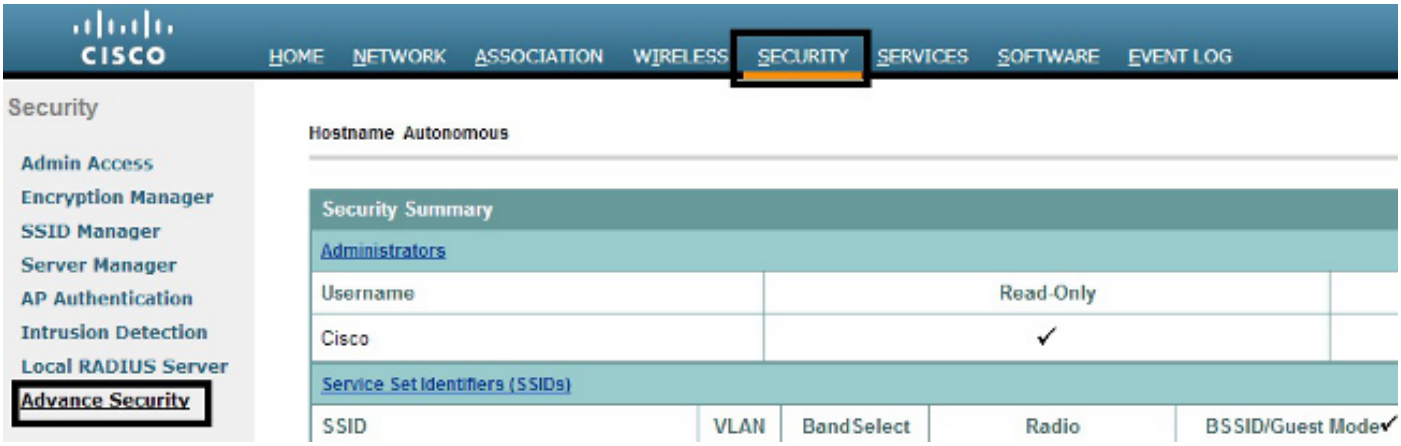
> **注:** CLI を使用した設定についての詳細は、シスコの記事『アクセス ポイント ACL フィルタの設定例』（英語）を参照してください。

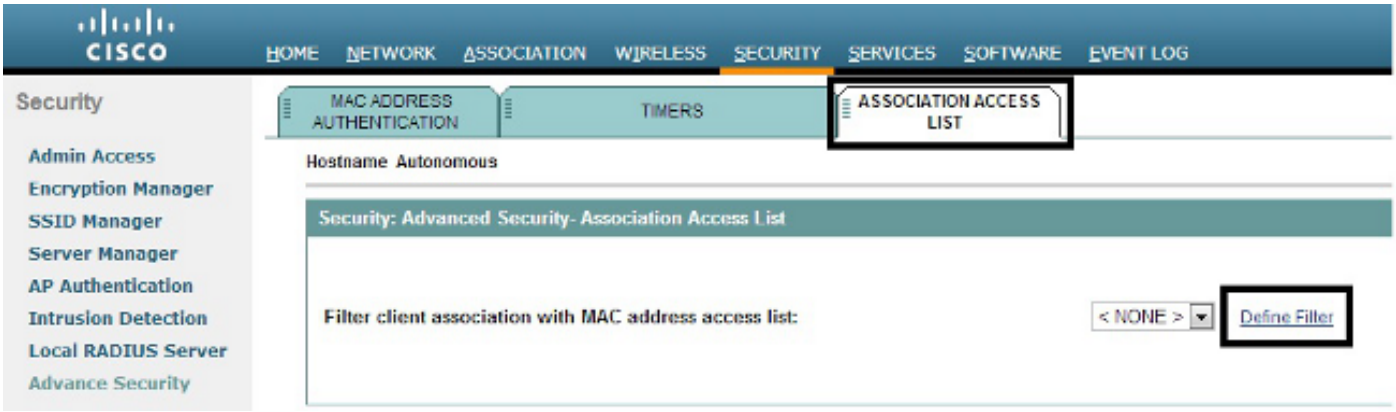
設定

このセクションでは、GUI を使用して Cisco Aironet AP 上で ACL ベースのフィルタを設定する方法について説明します。

ACL の作成場所

[Security] > [Advance Security] に移動します。 [Association Access List] タブを選択し、[Define Filter] をクリックします。



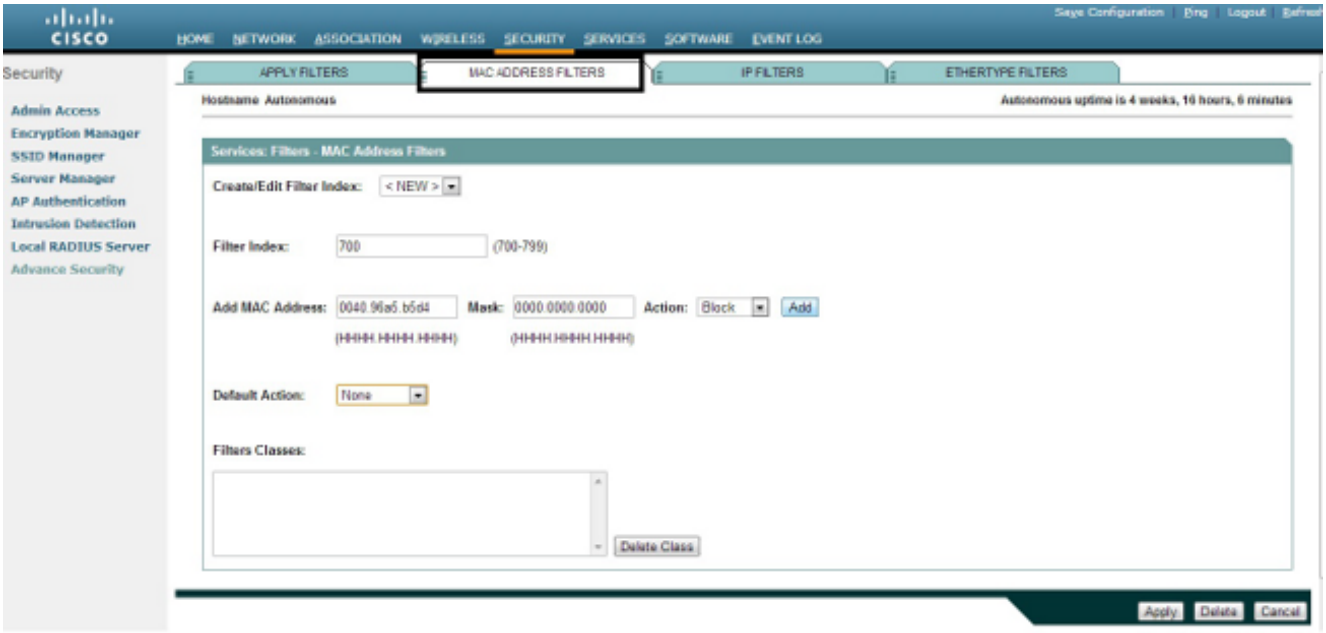


MAC アドレス フィルタ

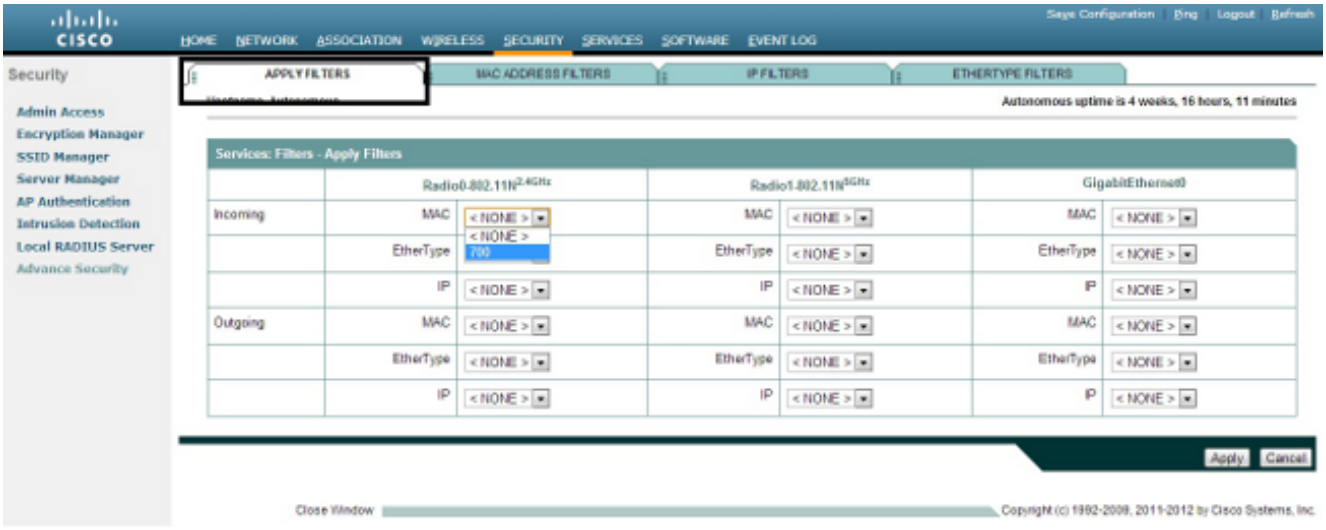
MAC アドレスベースのフィルタを使用すると、ハードコードされた MAC アドレスに基づくクライアント デバイスのフィルタリングを行うことができます。 クライアントが MAC ベースのフィルタでアクセスを拒否されると、そのクライアントは AP と関連付けできません。 MAC アドレスのフィルタによって、特定の MAC アドレスへ送受信されるユニキャストおよびマルチキャストのパケットの転送を、許可または禁止することができます。

この例は、MAC アドレスが **0040.96a5.b5d4** のクライアントをフィルタリングするために、GUI を使用して MAC ベースのフィルタを設定する方法を説明しています。

1. MAC アドレスの **ACL 700** を作成します。 この ACL では、クライアント **0040.96a5.b5d4** が AP に関連付けられるのを禁止します。



2. このフィルタをフィルタ クラスに追加するには、[Add] をクリックします。 また、デフォルトのアクションを [Forward All] または [Deny All] として定義することもできます。
3. [Apply] をクリックします。 **ACL 700** が作成されます。
4. **ACL 700** を無線インターフェイスに適用するには、[Apply Filters] セクションに移動します。 これで、入力または出力の無線または GigabitEthernet インターフェイスに、この ACL を適用できるようになります。



IP フィルタ

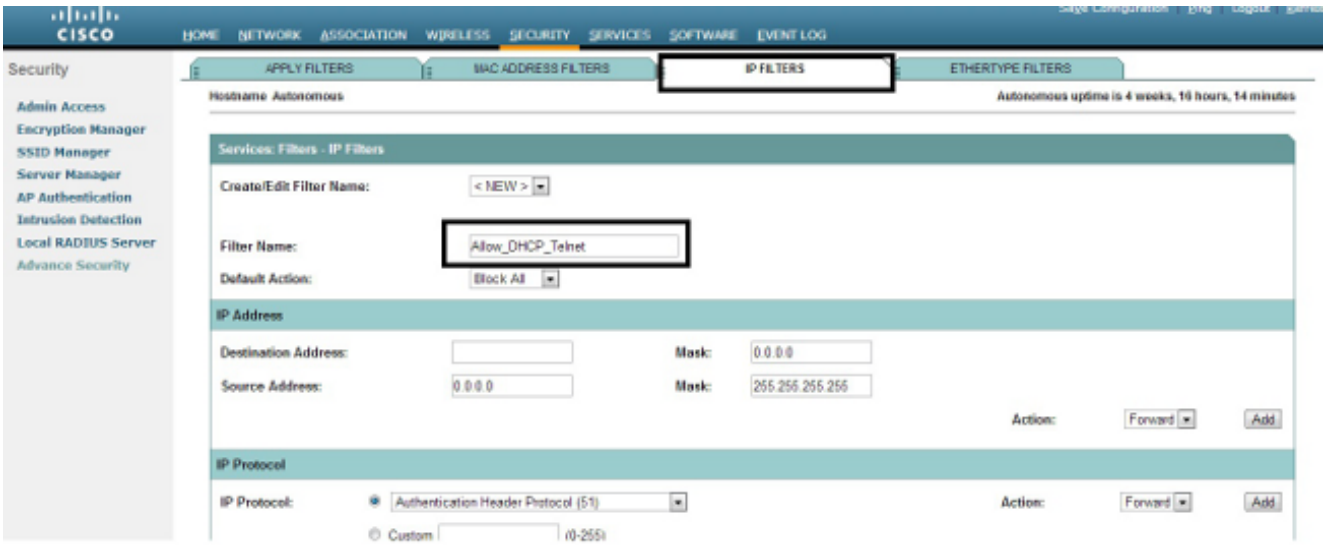
標準または拡張 ACL を使用すると、クライアント デバイスの WLAN ネットワークへの参加を、クライアントの IP アドレスに基づいて許可または禁止することができます。

この設定例では、拡張 ACL を使用しています。 拡張 ACL では、クライアントへの Telnet アクセスを許可する必要があります。 この WLAN ネットワークでは、他のプロトコルをすべて制限する必要があります。 また、クライアントは DHCP を使用して IP アドレスを取得します。 次のような拡張 ACL を作成する必要があります。

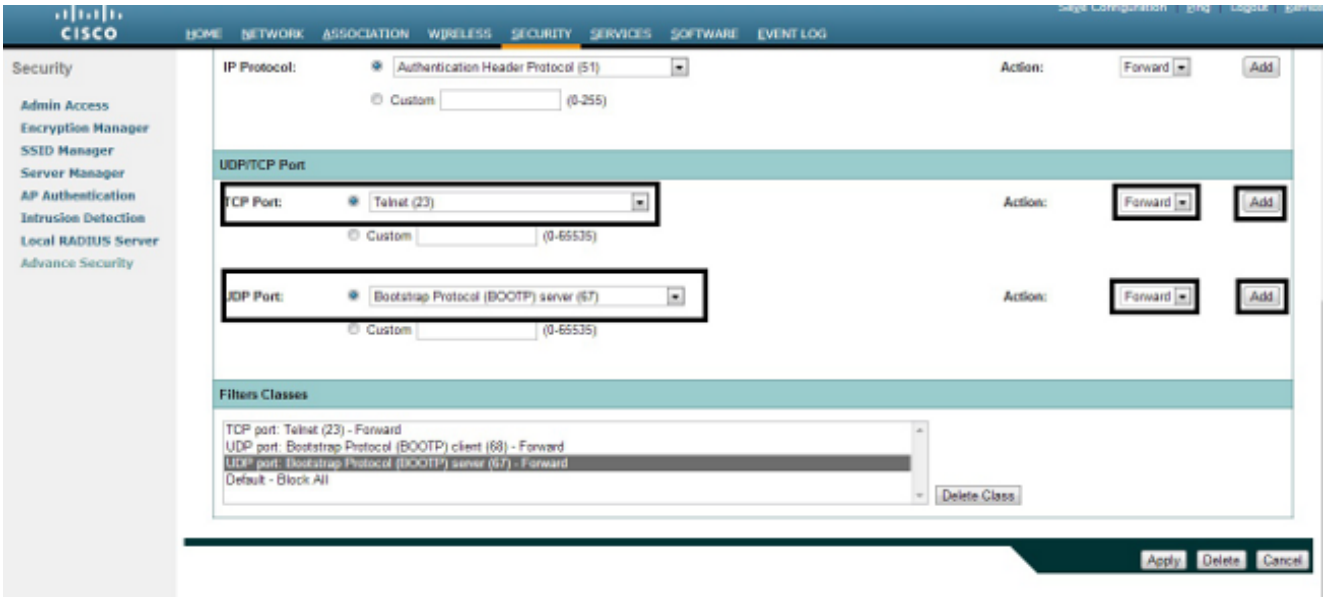
- DHCP と Telnet のトラフィックを許可する
- 他のすべてのタイプのトラフィックを拒否する

次の手順を実行して、拡張 ACL を作成します。

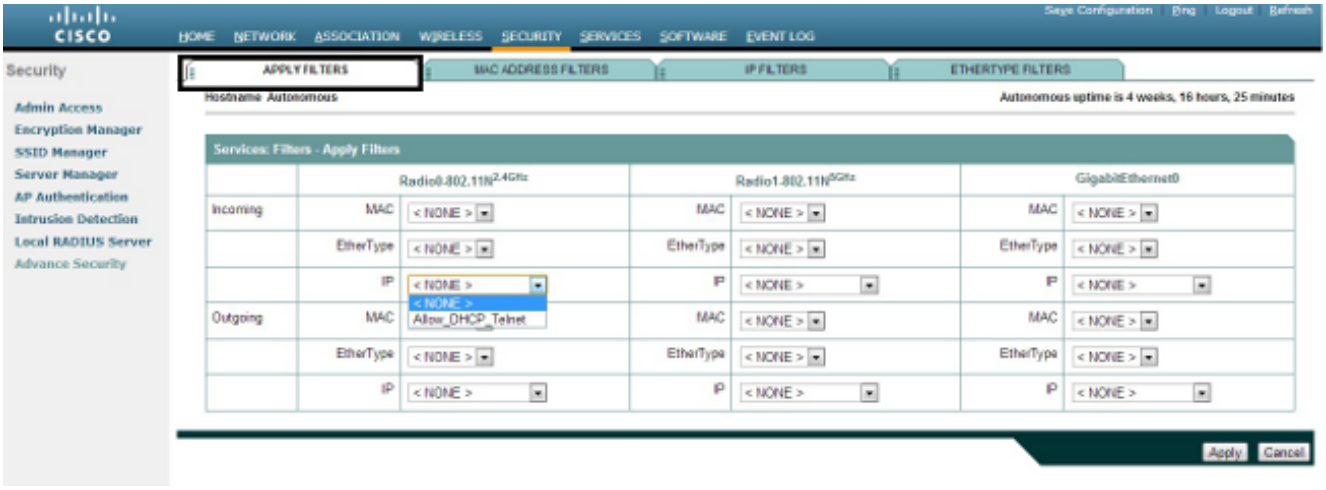
1. フィルタに名前を付け、[Default Action] ドロップダウン リストから [Block All] を選択します。これは、残りのトラフィックをブロックする必要があるためです。



2. [TCP Port] ドロップダウン リストから [Telnet] を選択し、[UDP Port] ドロップダウン リストから [BOOTP client & BOOTP server] を選択します。



3. [Apply] をクリックします。 IPフィルタ **Allow_DHCP か。_Telnet は**今作成され、着信か発信無線または GigabitEthernet インターフェイスにこの ACL を適用できます。

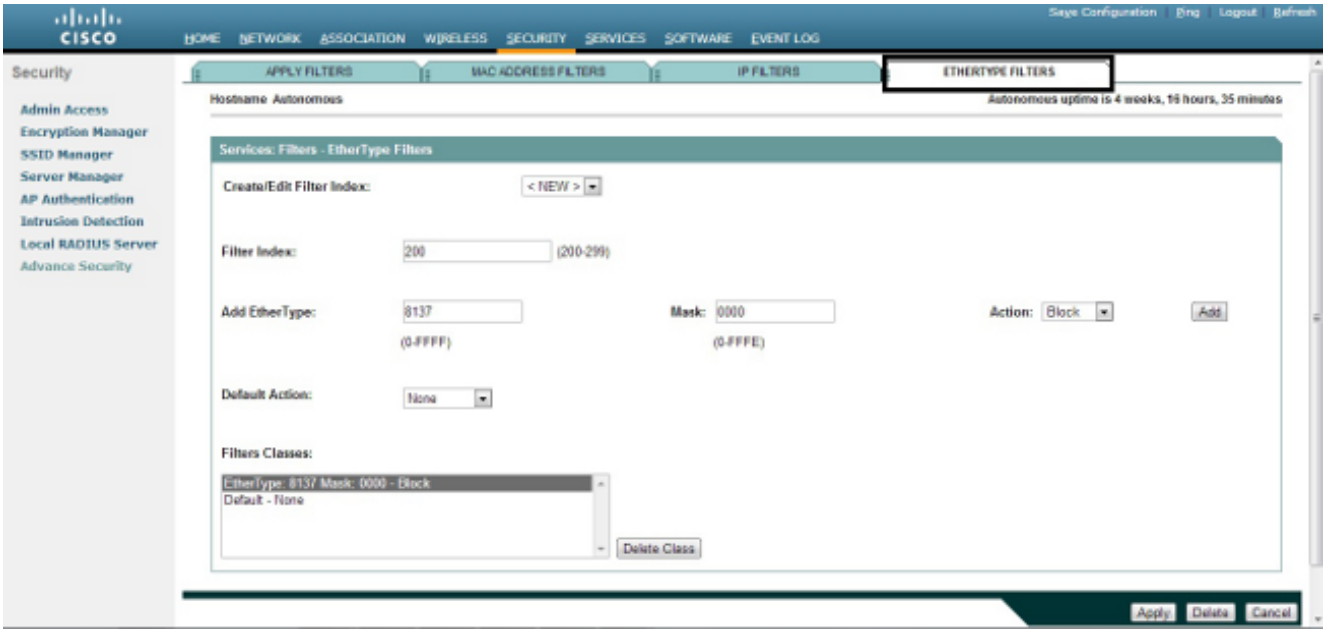


Ethertype フィルタ

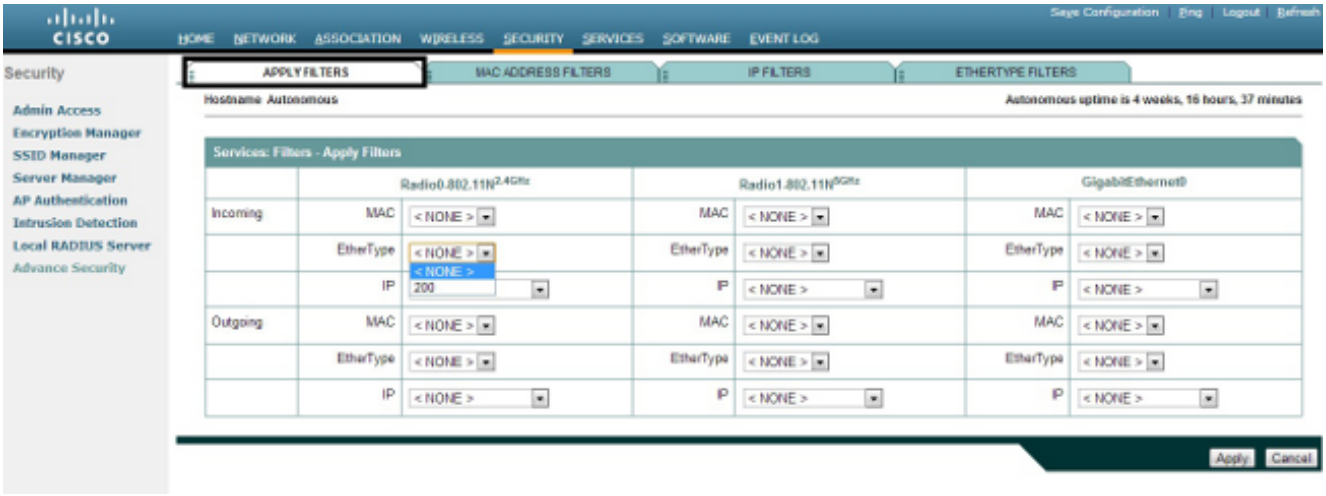
Ethertype フィルタを使用すると、Cisco Aironet AP で Internetwork Packet Exchange（IPX）トラフィックをブロックできます。 これが役立つ一般的な状況は、大規模な企業ネットワークで時々発生する、IPX サーバのブロードキャストがワイヤレス リンクを抑制する場合です。

IPX トラフィックをブロックするフィルタを設定して適用するには、次の手順を実行してください。

1. [Ethertype Filters] タブをクリックします。
2. [Filter Index] フィールドで、200 ~ 299 の範囲の番号でフィルタ名を設定します。 ユーザが割り当てた番号でフィルタの ACL が作成されます。
3. [Add Ethertype] フィールドに **8137** と入力します。
4. [Mask] フィールドの Ethertype のマスクは、デフォルト値のままにします。
5. アクション メニューから [Block] を選択し、[Add] をクリックします。



6. [Filters Classes] リストから Ethertype を削除するには、その Ethertype を選択して [Delete Class] をクリックします。 上記の手順を繰り返して、フィルタにタイプ **8138**、**00ff**、**00e0** を追加します。 これで、入力または出力の無線または GigabitEthernet インターフェイスに、この ACL を適用できるようになります。


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