Konfigurationsbeispiel für ACL-Filter auf Aironet APs

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ACL-basierte Filter (Access Control List) auf Cisco Aironet Access Points (APs) mithilfe der GUI konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Konfiguration einer Wireless-Verbindung unter Verwendung eines Aironet AP und eines Aironet 802.11 a/b/g Client Adapter
- ACLs

Verwendete Komponenten

In diesem Dokument werden APs der Serie Aironet 1040 verwendet, auf denen die Cisco IOS® Software, Version 15.2(2)JB, ausgeführt wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Sie können auf den APs Filter verwenden, um folgende Aufgaben durchzuführen:

- Beschränken des Zugriffs auf das WLAN
- Zusätzliche Wireless-Sicherheit

Sie können verschiedene Arten von Filtern verwenden, um Datenverkehr auf der Grundlage von:

- Spezifische Protokolle
- Die MAC-Adresse des Client-Geräts
- Die IP-Adresse des Client-Geräts

Sie können auch Filter aktivieren, um den Datenverkehr von Benutzern im LAN einzuschränken. IP-Adressen- und MAC-Adressfilter erlauben oder verbieten die Weiterleitung von Unicast- und Multicast-Paketen, die von oder an bestimmte IP- oder MAC-Adressen gesendet werden.

Protokollbasierte Filter bieten eine detailliertere Möglichkeit, den Zugriff auf bestimmte Protokolle über die Ethernet- und Funkschnittstellen des Access Points zu beschränken. Sie können eine der folgenden Methoden verwenden, um die Filter auf den APs zu konfigurieren:

- Weboberfläche
- CLI

In diesem Dokument wird die Verwendung von ACLs zum Konfigurieren von Filtern über die GUI erläutert.

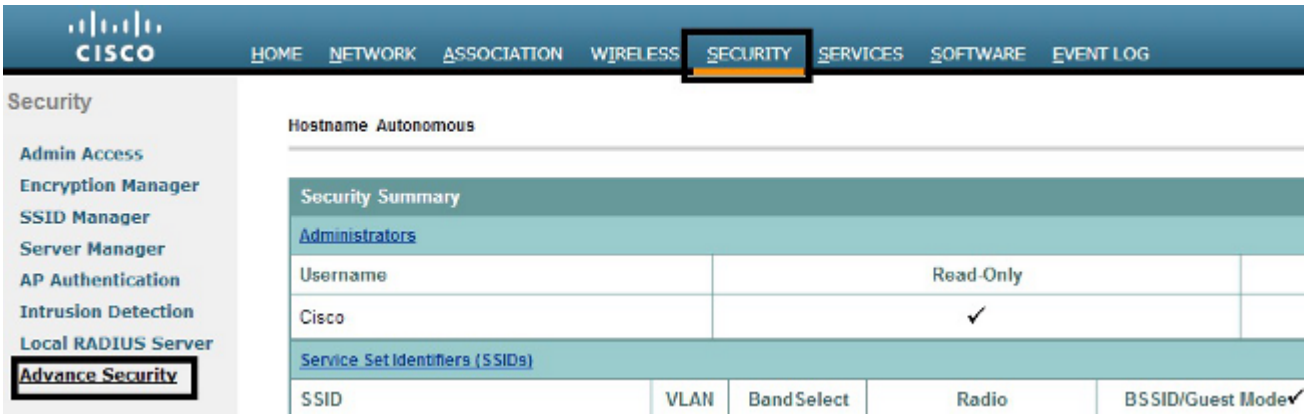
> **Hinweis**: Weitere Informationen zur Konfiguration über die CLI finden Sie im Cisco Artikel Access Point ACL Filter Configuration Example.

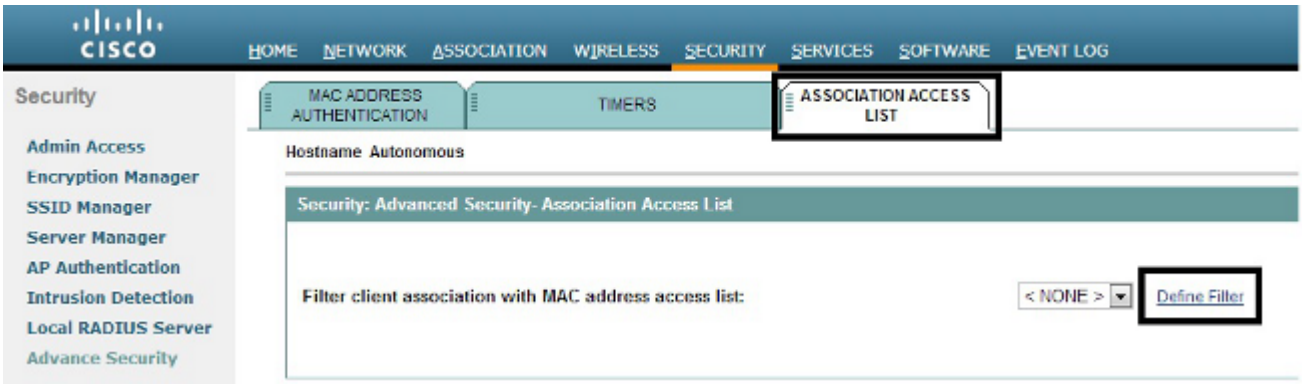
Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie ACL-basierte Filter auf Cisco Aironet APs mithilfe der GUI konfigurieren.

Erstellen von ACLs

Navigieren Sie zu **Sicherheit** > **Erweiterte Sicherheit**. Wählen Sie die Registerkarte **Association Access List** aus, und klicken Sie auf **Define Filter**:



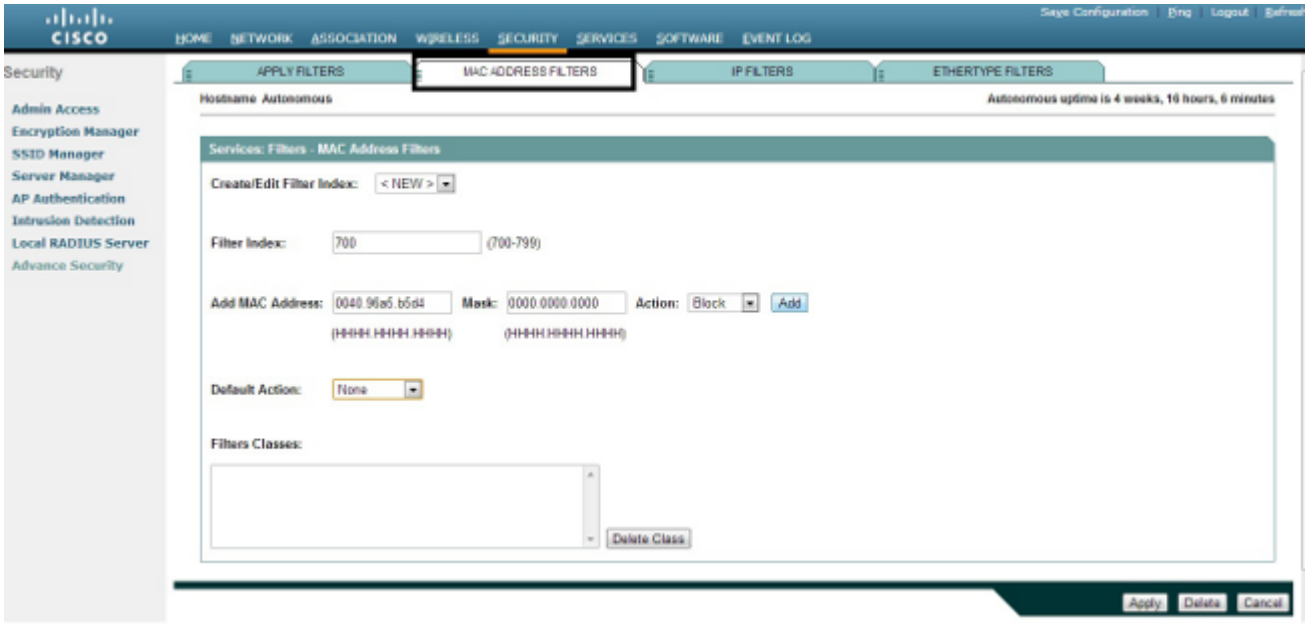


MAC-Adressfilter

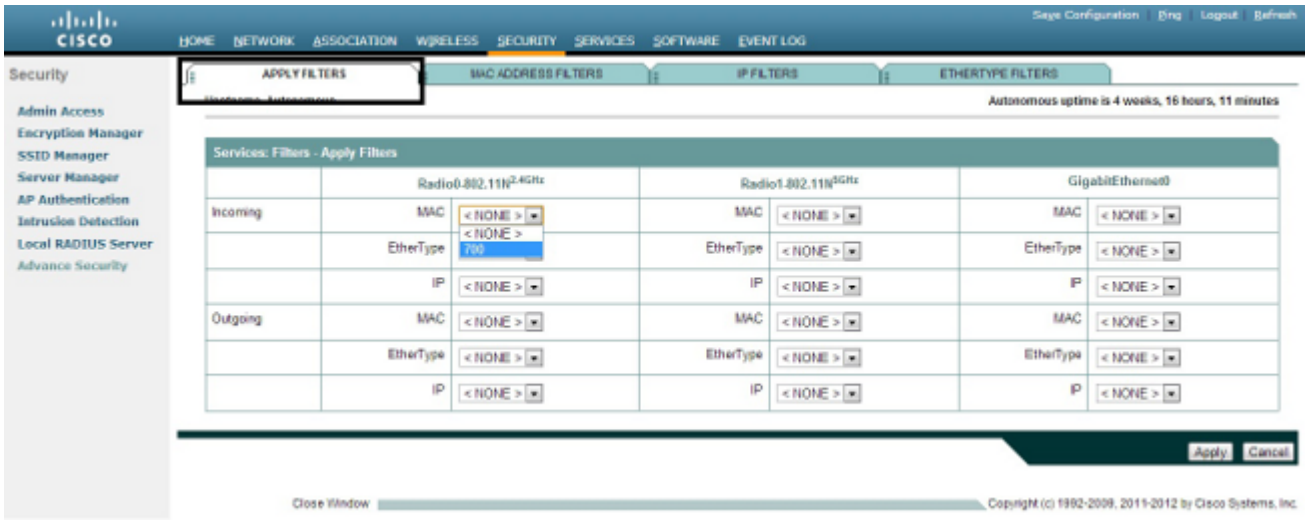
Sie können MAC-Adressbasierte Filter verwenden, um Client-Geräte anhand der hartcodierten MAC-Adresse zu filtern. Wenn einem Client der Zugriff über einen MAC-basierten Filter verweigert wird, kann der Client keine Verbindung zum AP herstellen. MAC-Adressfilter erlauben oder verhindern die Weiterleitung von Unicast- und Multicast-Paketen, die entweder von bestimmten MAC-Adressen gesendet oder an bestimmte MAC-Adressen adressiert werden.

In diesem Beispiel wird veranschaulicht, wie ein MAC-basierter Filter über die Benutzeroberfläche konfiguriert wird, um den Client mit der MAC-Adresse **0040.96a5.b5d4** zu filtern:

1. Erstellen Sie die **ACL 700 für** die MAC-Adresse. Mit dieser ACL kann der Client **0040.96a5.b5d4** keine Verbindung mit dem Access Point herstellen.



2. Klicken Sie auf **Hinzufügen**, um diesen Filter den Filterklassen hinzuzufügen. Sie können die Standardaktion auch als **Alle weiterleiten** oder **Alle verweigern** definieren.
3. Klicken Sie auf Apply (Anwenden). **ACL 700** wurde erstellt.
4. Um **ACL 700** auf eine Funkschnittstelle anzuwenden, navigieren Sie zum Abschnitt **Filter anwenden**. Sie können diese ACL jetzt auf eine Funkschnittstelle (Eingang oder Ausgang) oder eine GigabitEthernet-Schnittstelle anwenden.



IP-Filter

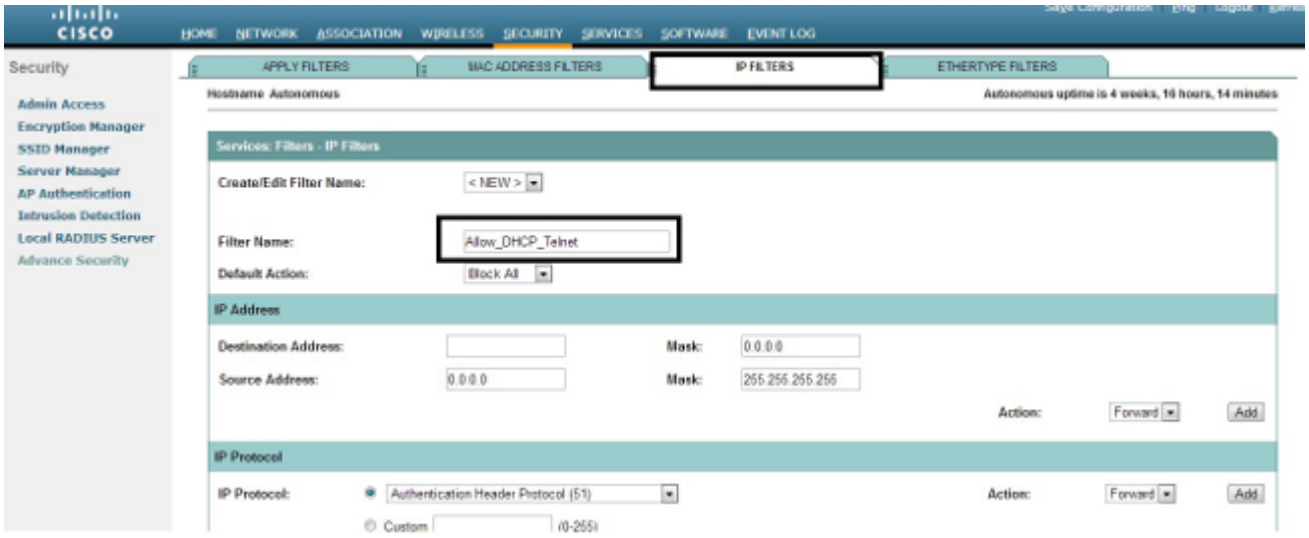
Sie können standardmäßige oder erweiterte Zugriffskontrolllisten verwenden, um den Zugriff von Client-Geräten auf das WLAN basierend auf der IP-Adresse des Clients zu erlauben oder zu verweigern.

In diesem Konfigurationsbeispiel werden erweiterte Zugriffskontrolllisten verwendet. Die erweiterte ACL muss den Telnet-Zugriff auf die Clients zulassen. Sie müssen alle anderen Protokolle im WLAN einschränken. Außerdem verwenden die Clients DHCP, um die IP-Adresse abzurufen. Sie müssen eine erweiterte ACL erstellen, die:

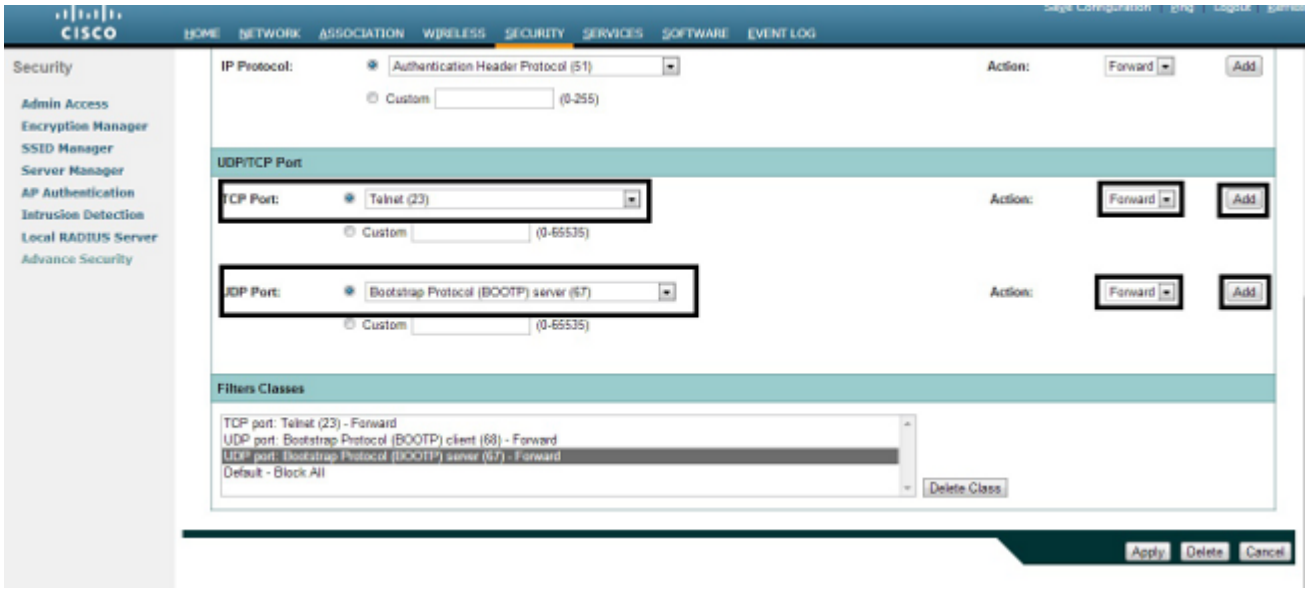
- Ermöglicht DHCP- und Telnet-Datenverkehr
- Verweigert alle anderen Datenverkehrstypen

Gehen Sie wie folgt vor, um die Datei zu erstellen:

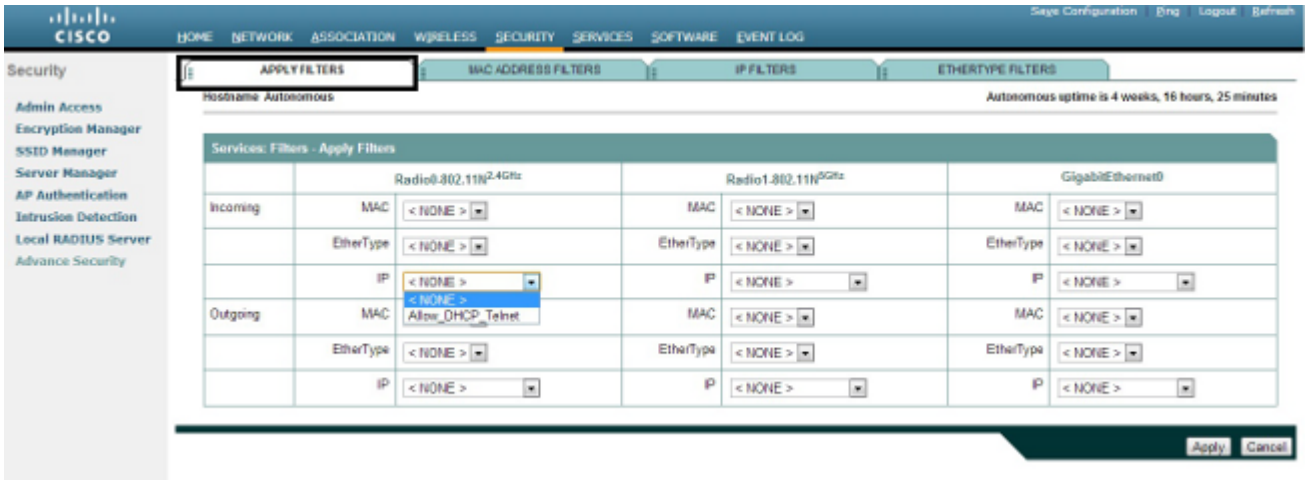
1. Geben Sie dem Filter einen Namen, und wählen Sie **Block All (Alle blockieren**) in der Dropdown-Liste **Default Action (Standardaktion**) aus, da der verbleibende Datenverkehr blockiert werden muss:



2. Wählen Sie Telnet aus der Dropdown-Liste **TCP Port (TCP-Port**) und **BOOTP Client** & **BOOTP Server** aus der Dropdown-Liste **UDP Port (**BOOTP-**Client** und **BOOTP-Server**) aus:



3. Klicken Sie auf **Apply (Anwenden).** Der IP-Filter **Allow_DHCP?_Telnet** wurde erstellt, und Sie können diese ACL auf eine eingehende oder ausgehende Radio- oder GigabitEthernet-Schnittstelle anwenden.

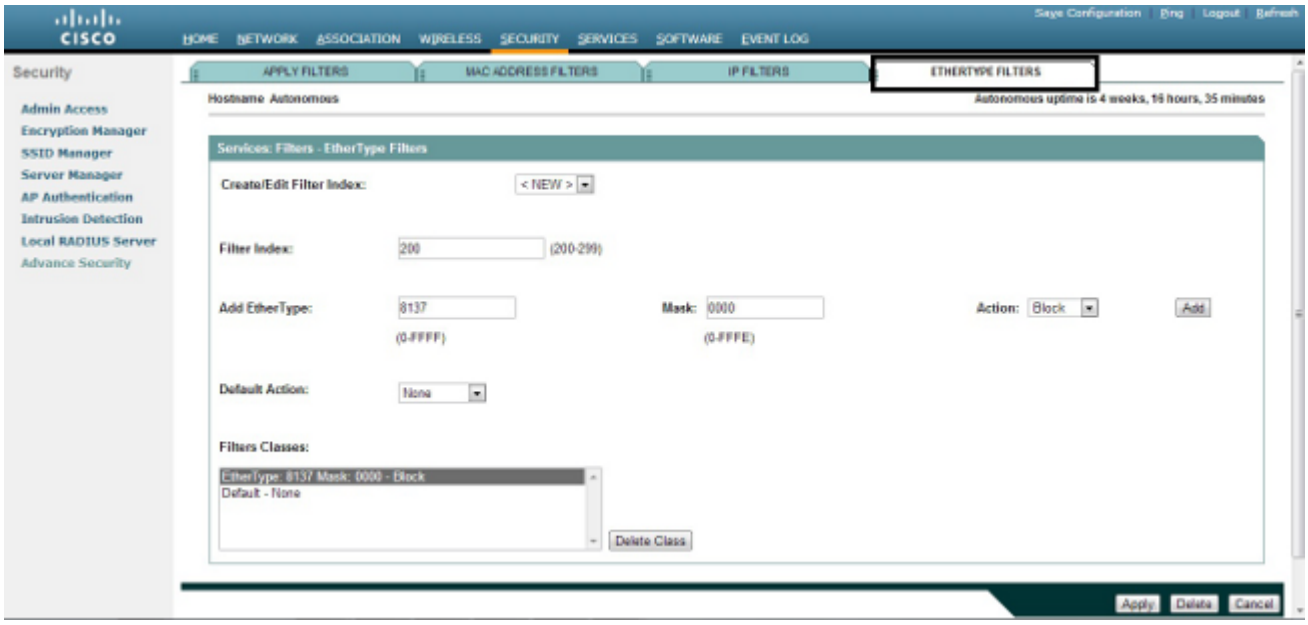


Ethertype-Filter

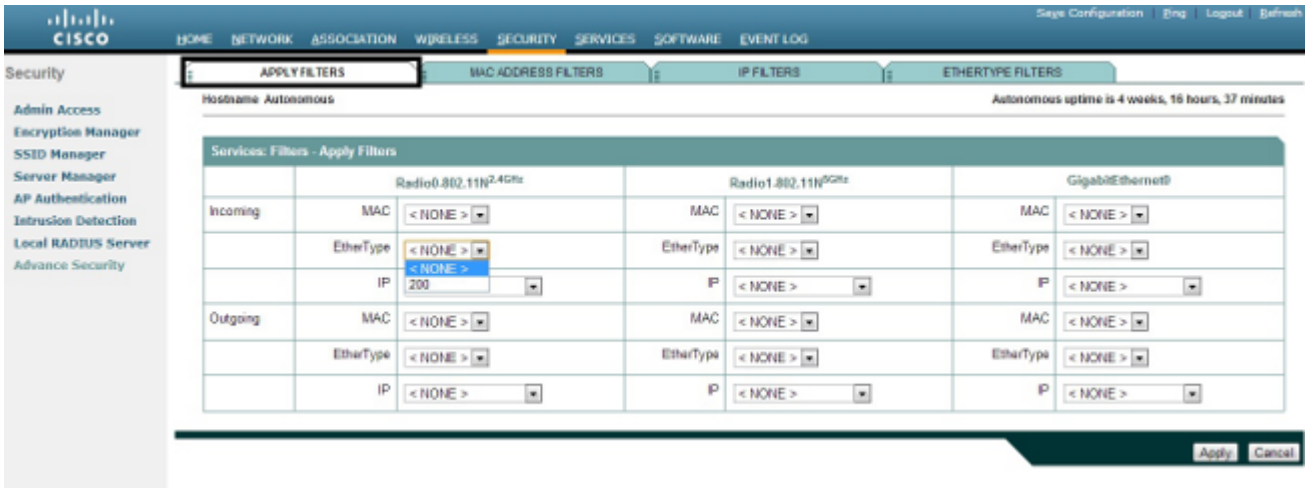
Sie können Ethertype-Filter verwenden, um IPX-Datenverkehr (Internetwork Packet Exchange) auf dem Cisco Aironet AP zu blockieren. Eine typische Situation, in der dies nützlich ist, ist, wenn die Wireless-Verbindung durch den IPX-Server unterbrochen wird, was manchmal in einem großen Unternehmensnetzwerk der Fall ist.

Gehen Sie wie folgt vor, um einen Filter zu konfigurieren und anzuwenden, der IPX-Datenverkehr blockiert:

1. Klicken Sie auf die Registerkarte **Ethertype Filters (Ethertypfilter**).
2. Geben Sie im Feld **Filterindex** dem Filter einen Namen mit einer Zahl zwischen 200 und 299. Durch die Nummer, die Sie zuweisen, wird eine ACL für den Filter erstellt.
3. Geben Sie in das Feld **Ethertype hinzufügen** den Wert **8137 ein**.
4. Lassen Sie die Maske für den Ethertype im **Maskenfeld** auf dem Standardwert.
5. Wählen Sie im Menü Aktion die Option **Block** aus, und klicken Sie auf **Hinzufügen**.



6. Um den Ethertype aus der Liste Filterklassen zu entfernen, wählen Sie ihn aus, und klicken Sie auf **Klasse löschen**. Wiederholen Sie die vorherigen Schritte, und fügen Sie dem Filter die Typen **8138**, **00ff** und **00e0** hinzu. Sie können diese ACL jetzt auf eine Funkschnittstelle (Eingang oder Ausgang) oder eine GigabitEthernet-Schnittstelle anwenden.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.