Фильтры ACL на примере конфигурации AP Aironet

Содержание

Введение

Этот документ описывает, как настроить Список контроля доступа (ACL) - основанные фильтры на точках доступа Cisco Aironet (AP) с использованием GUI.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- Конфигурация беспроводного соединения с использованием AP Aironet и Клиентского адаптера a/b/g 802.11 Aironet
- ACL

Используемые компоненты

Этот документ использует Aironet AP серии 1040, которые выполняют JB Выпуска 15.2 (2) программного обеспечения Cisco IOS.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Можно использовать фильтры на AP для выполнения этих задач:

- Ограничьте доступ к сети (WLAN) беспроводной локальной сети
- Предоставьте дополнительный уровень безопасности беспроводной связи

Можно использовать различные типы фильтров чтобы к трафику фильтрации на основе:

- Определенные протоколы
- MAC-адрес устройства клиента
- IP-адрес устройства клиента

Можно также включить фильтры для ограничения трафика от пользователей на проводной LAN. IP-адрес и Фильтры MAC - адреса позволяют или запрещают передачу индивидуальной рассылки и пакетов групповой адресации, которые передаются или от определенного IP или MAC-адресов.

Основанные на протоколе фильтры предоставляют более гранулированный способ ограничить доступ к определенным протоколам через Ethernet и радиоинтерфейсы AP. Можно использовать любой из этих методов для настройки фильтров на AP:

- Веб-GUI
- CLI

Этот документ объясняет, как использовать ACL для настройки, проникает в GUI.

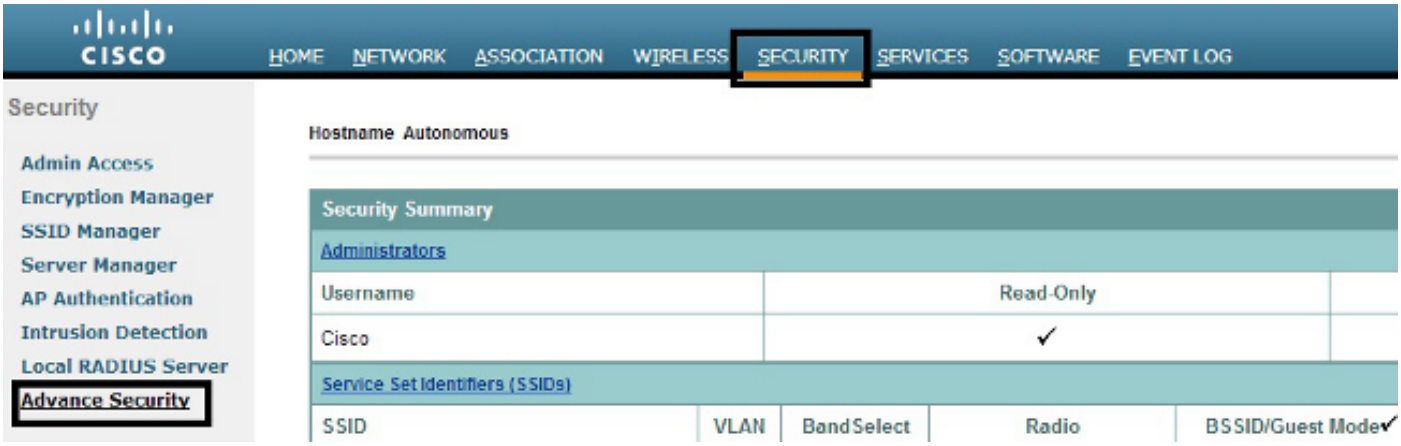
> **Примечание:** Для получения дополнительной информации о конфигурации посредством использования CLI, обратитесь к статье ACL Filter Configuration Example Cisco точки доступа.

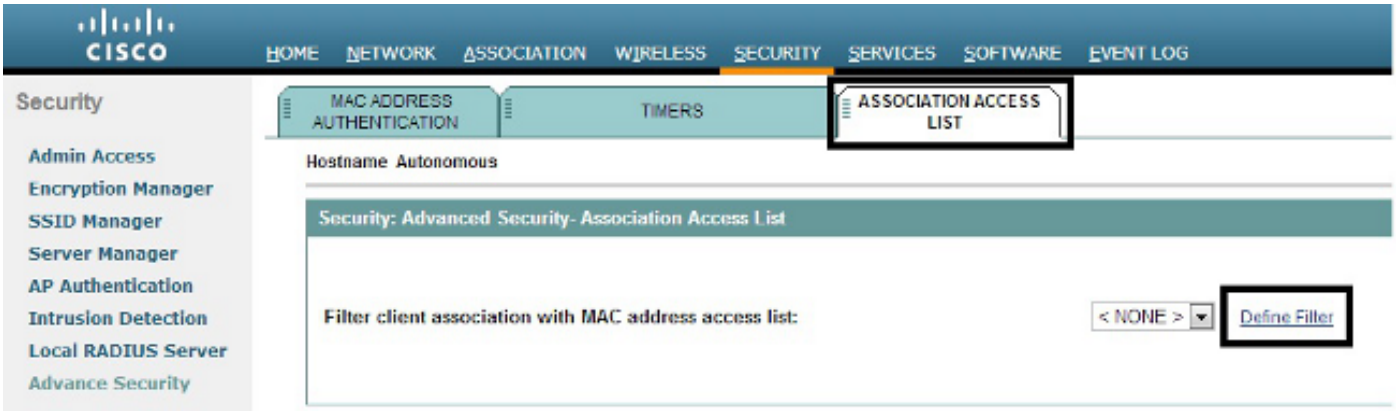
Настройка

В этом разделе описывается настроить основанные на ACL фильтры на AP Cisco Aironet с использованием GUI.

Где создать ACL

Перейдите к **Безопасности> Безопасность Усовершенствования**. Выберите вкладку **Association Access List** и нажмите **Define Filter**:



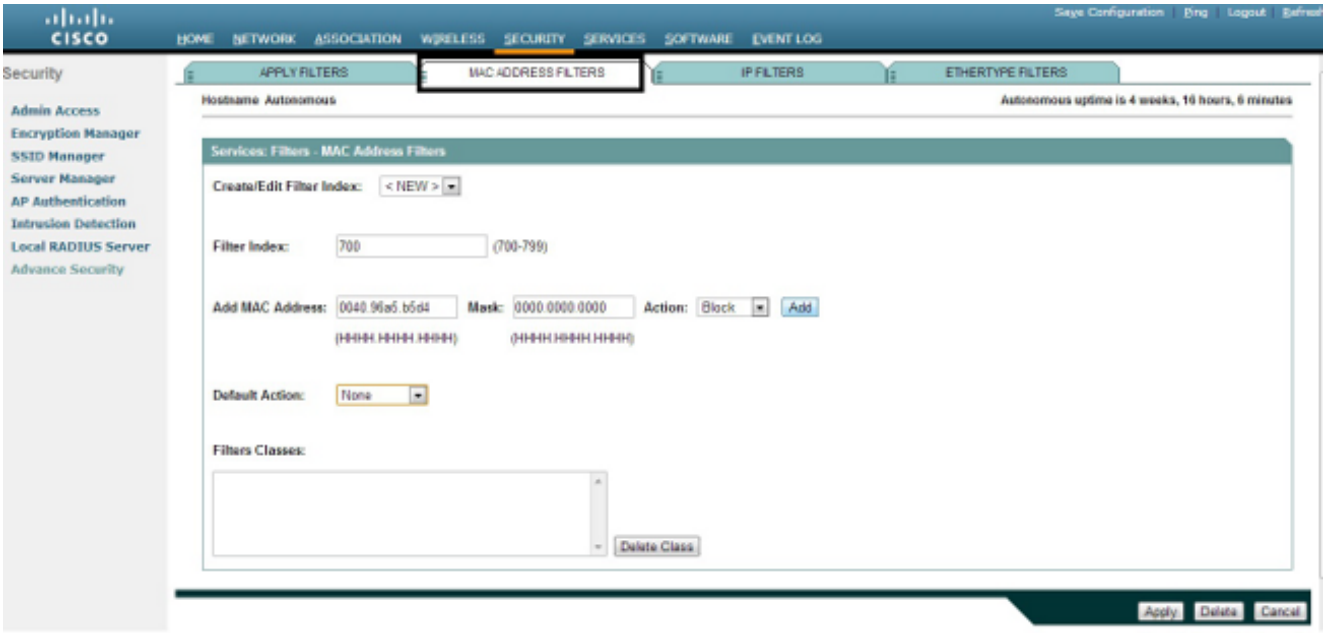


Фильтры MAC - адреса

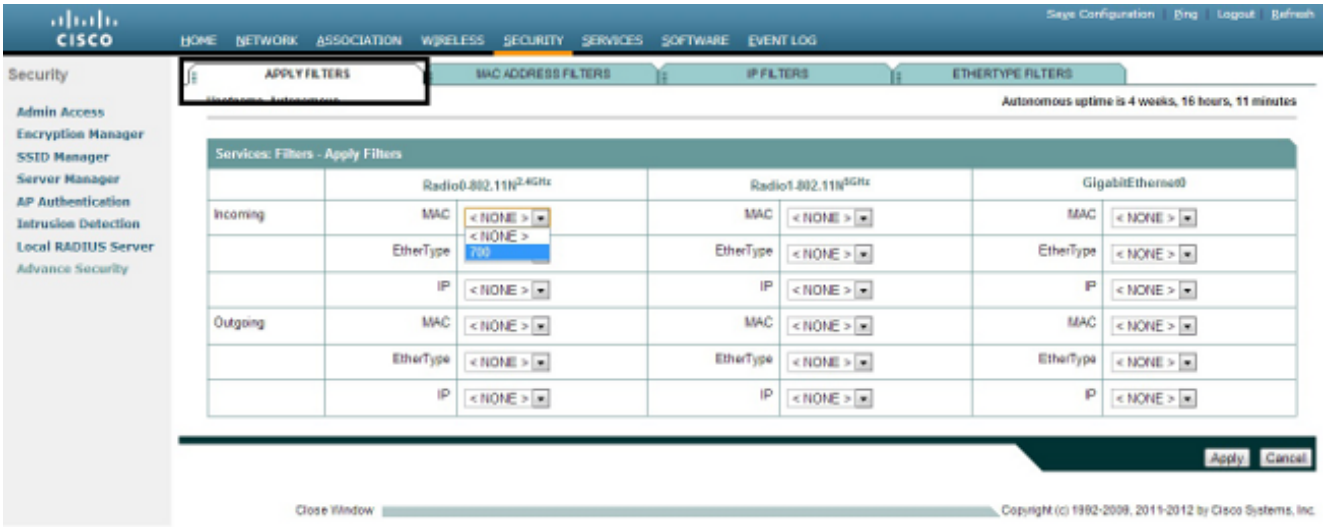
Можно использовать MAC, на основе адреса фильтрует для фильтрации устройств клиента на основе жестко закодированного MAC-адреса. Когда клиенту запрещают доступ через на основе MAC фильтр, клиент не может связаться с AP. Фильтры MAC - адреса позволяют или запрещают передачу индивидуальной рассылки и пакетов групповой адресации, или передаваемых от, или адресованный, определенные MAC-адреса.

Данный пример иллюстрирует, как настроить, на основе MAC проникают в GUI для фильтрации клиента с MAC-адресом **0040.96a5.b5d4**:

1. Создайте **MAC-адрес ACL 700**. Этот ACL не позволяет клиентскому **0040.96a5.b5d4** связываться с AP.



2. **Нажмите Add** для добавления этого фильтра к Классам Фильтров. Можно также определить действие по умолчанию как **Вперед Все** или **Запретить Все**.
3. **Щелкните "Применить". ACL 700** теперь создан.
4. Для применения **ACL 700** к радиоинтерфейсу перейдите к **Применять** разделу **Фильтров**. Можно теперь применить этот ACL к поступлению или исходящему интерфейсу Радио или GigabitEthernet.



Фильтры IP

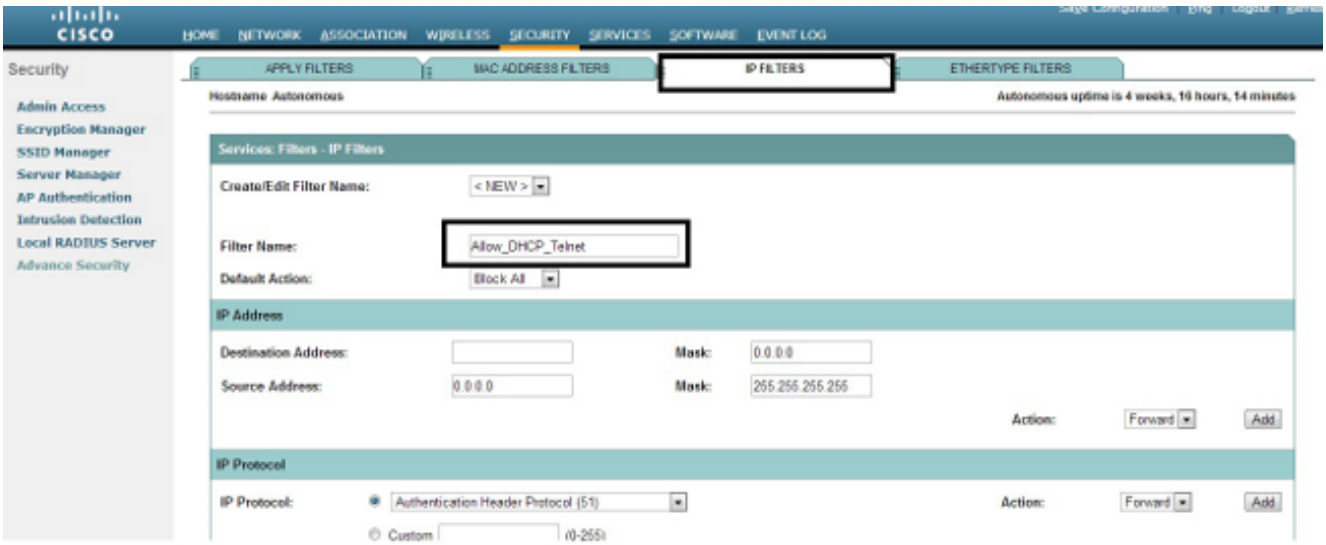
Можно использовать стандарт или расширенные списки ACL, чтобы позволить или запретить запись устройств клиента в сеть WLAN на основе IP-адреса клиента.

Этот пример конфигурации использует расширенные списки ACL. Расширенный список ACL должен предоставить доступ Telnet клиентам. Необходимо ограничить все другие протоколы на сети WLAN. Кроме того, клиенты используют DHCP для получения IP-адреса. Необходимо создать расширенный список ACL что:

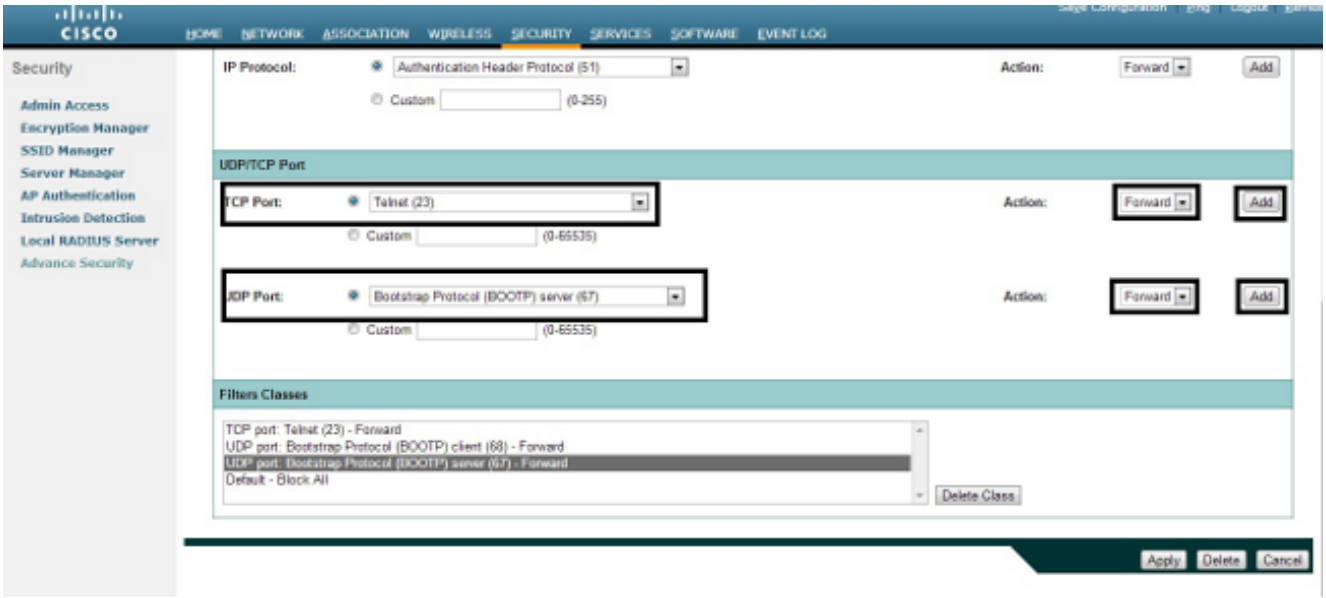
- Позволяет трафик DHCP и трафик Telnet
- Запрещает все другие типы трафика

Выполните эти шаги для создания его:

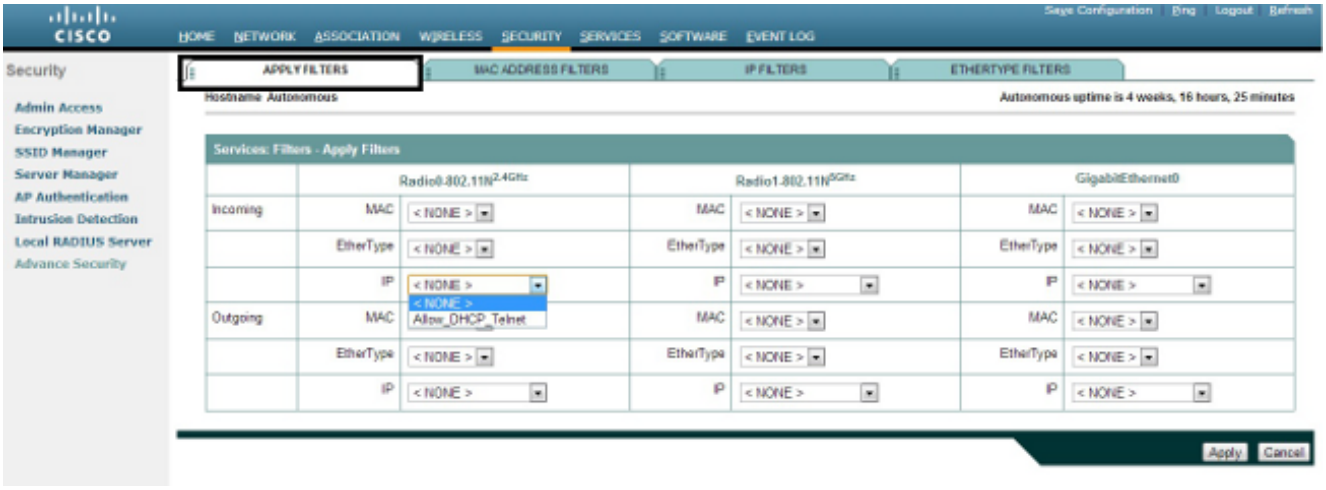
1. Назовите фильтр и выберите **Block All** от выпадающего списка **Действия по умолчанию**, так как должен быть заблокирован оставшийся трафик:



2. Выберите **Telnet** от выпадающего списка **Порта TCP**, и **Клиента BOOTP** и **сервер BOOTP** от выпадающего списка **порта UDP**:



3. **Щелкните "Применить".** Фильтр IP **Allow_DHCP? _Telnet** теперь создан, и можно применить этот ACL к поступлению или исходящему интерфейсу Радио или GigabitEthernet.

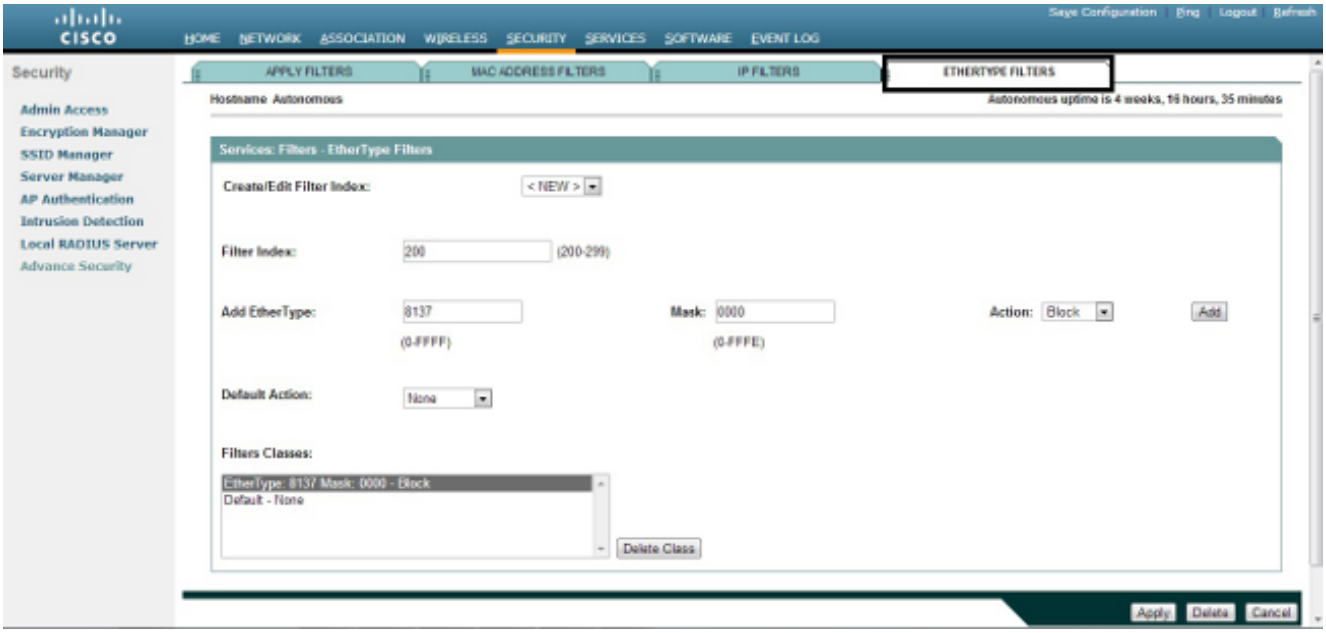


Фильтры Ethertype

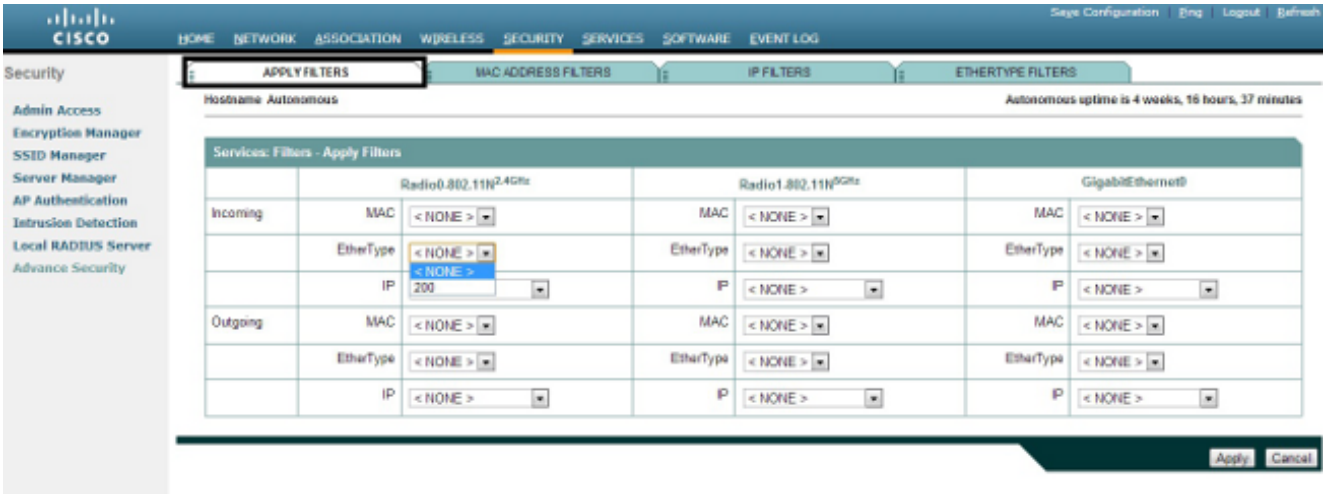
Можно использовать фильтры Ethertype для блокирования трафика Межсетевого пакетного обмена (IPX) на точке доступа Cisco Aironet. Типичная ситуация, где это полезно, - когда широковещательные сообщения сервера IPX дросселируют беспроводное соединение, которое иногда происходит в большой корпоративной сети.

Выполните эти шаги, чтобы настроить и применить фильтр, который блокирует трафик IPX:

1. Нажмите вкладку **Ethertype Filters**.
2. В **Поле индекса Фильтра** назовите фильтр с номером от 200 до 299. Номер, который вы назначаете, создает ACL для фильтра.
3. Войдите **8137** в поле **Add Ethertype**.
4. Оставьте маску для Ethertype в **поле Mask** в значении по умолчанию.
5. Выберите **Block** из меню Действие и **нажмите Add**.



6. Для удаления Ethertype из списка Классов Фильтров выберите его и нажмите **Delete Class**. Повторите предыдущие шаги и добавьте **типы 8138, 00ff** и **00e0** к фильтру. Можно теперь применить этот ACL к поступлению или исходящему интерфейсу Радио или GigabitEthernet.


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