Aironet AP上的ACL過濾器配置示例

目錄

簡介

本檔案介紹如何使用GUI在Cisco Aironet存取點(AP)上設定存取控制清單(ACL)型過濾器。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 使用Aironet AP和Aironet 802.11 a/b/g客戶端介面卡配置無線連線
- ACL

採用元件

本檔案使用執行Cisco IOS®軟體版本15.2(2)JB的Aironet 1040系列AP。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

您可以在AP上使用過濾器來執行以下任務：

- 限制對無線LAN(WLAN)網路的訪問
- 提供額外的無線安全層

您可以使用不同型別的過濾器根據以下條件過濾流量：

- 特定通訊協定
- 客戶端裝置的MAC地址
- 客戶端裝置的IP地址

您也可以啟用篩選條件，以限制來自有線LAN上使用者的流量。IP地址和MAC地址過濾器允許或不允許轉發傳送到特定IP或MAC地址的單播和組播資料包。

基於協定的過濾器提供了一種更精細的方式，以限制通過AP的乙太網和無線電介面訪問特定協定。您可以使用以下任一方法在AP上設定過濾器：

- Web GUI
- CLI

本檔案將說明如何使用ACL透過GUI設定過濾器。

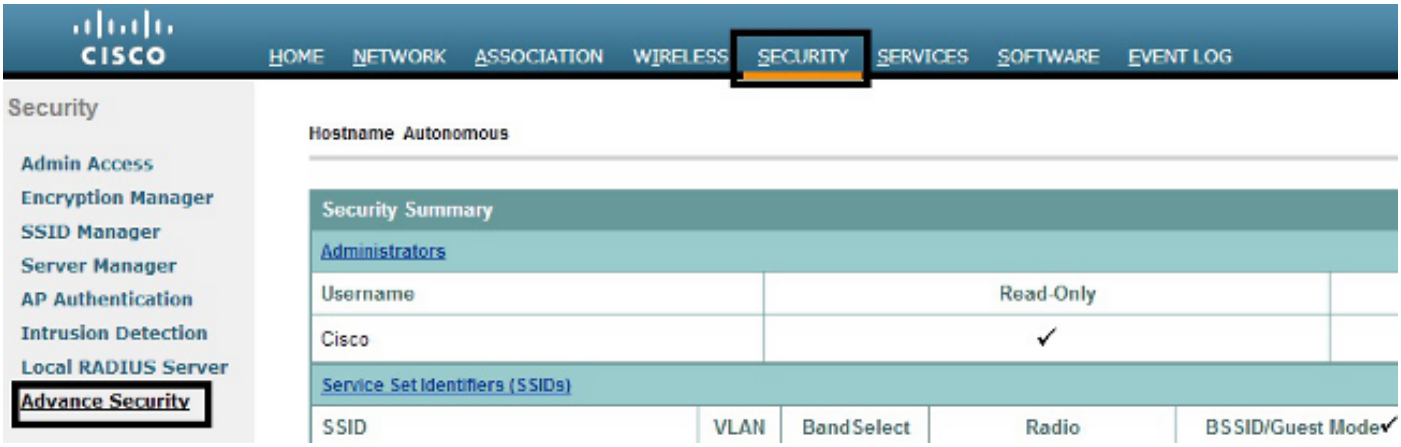
注意：有關使用CLI進行配置的詳細資訊，請參閱接入點ACL過濾器配置示例Cisco文章。

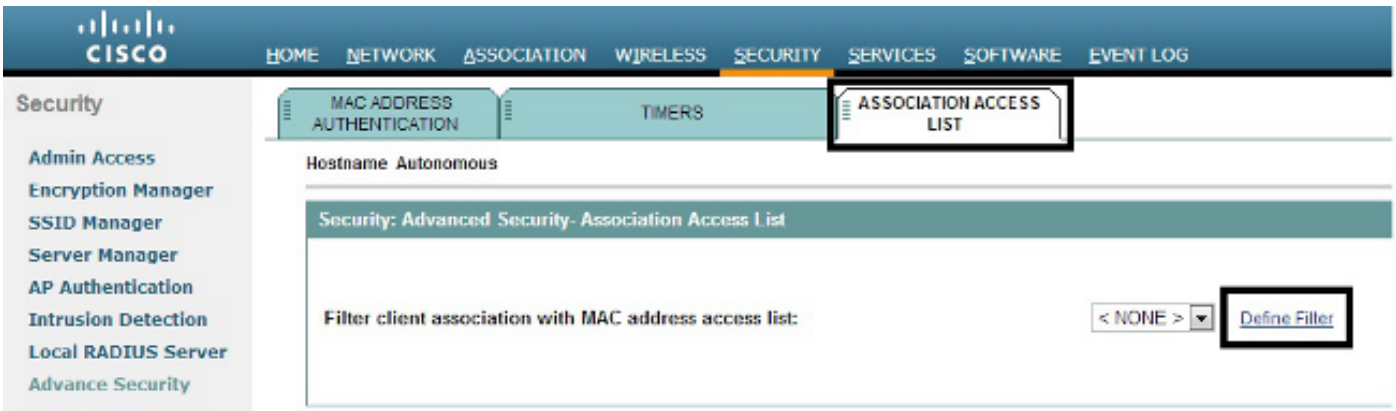
設定

本節介紹如何使用GUI在Cisco Aironet AP上配置基於ACL的過濾器。

建立ACL的位置

導覽至Security > Advanced Security。選擇Association Access List頁籤，然後按一下Define Filter:



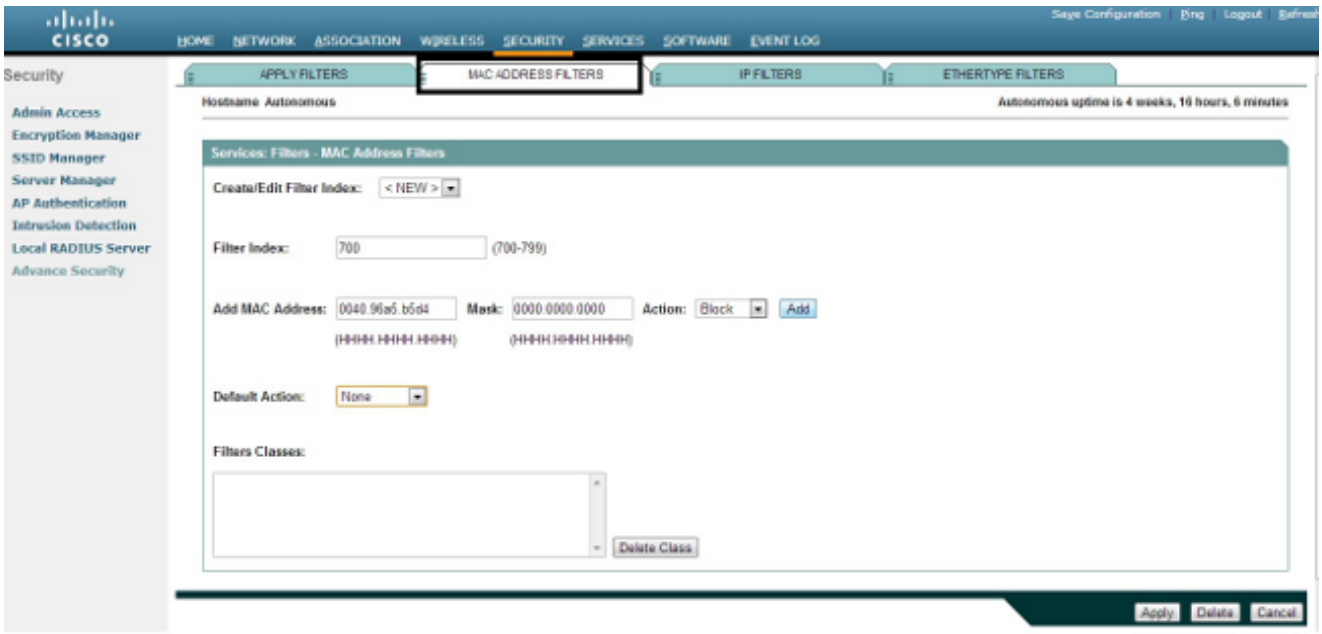


MAC位址過濾器

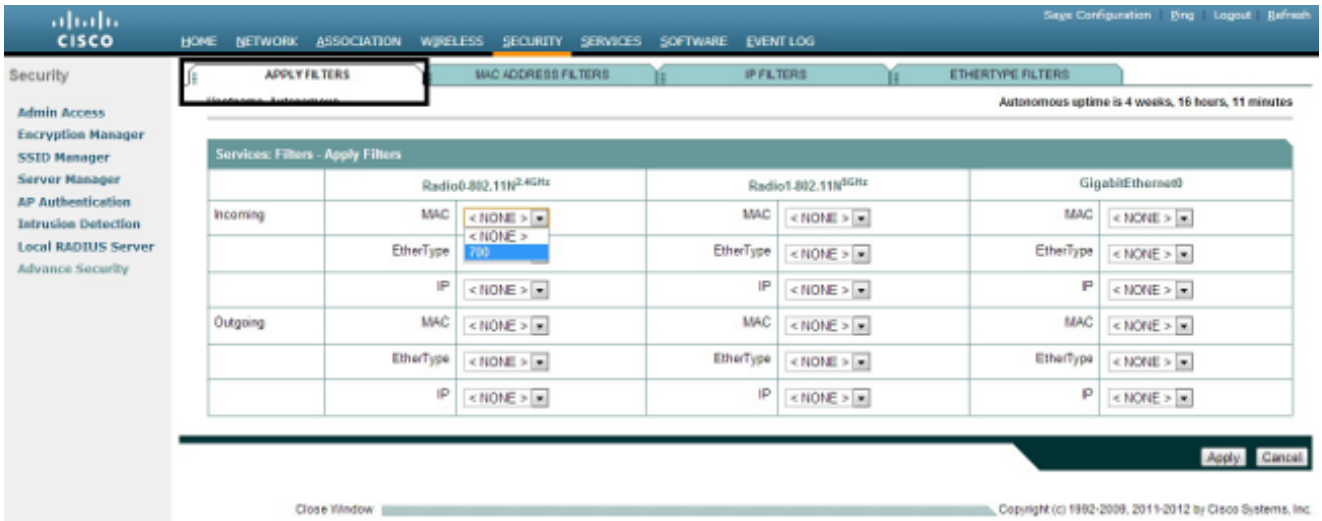
您可以使用基於MAC地址的過濾器來根據硬編碼MAC地址過濾客戶端裝置。當客戶端被拒絕通過基於MAC的過濾器訪問時，客戶端無法與AP關聯。MAC地址過濾器允許或不允許轉發從特定MAC地址傳送或發往特定MAC地址的單播和組播資料包。

此範例說明如何透過GUI設定基於MAC的過濾器，以便使用MAC位址0040.96a5.b5d4過濾使用者端：

1. 建立MAC地址ACL 700。此ACL不允許客戶端0040.96a5.b5d4與AP關聯。



2. 按一下Add以將此篩選器新增到篩選器類。您還可以將預設操作定義為全部轉發或全部拒絕。
3. 按一下「Apply」。ACL 700現已建立。
4. 若要將ACL 700套用到無線介面，請導覽至Apply Filters一節。現在，您可以將此ACL應用於傳入或傳出無線電或GigabitEthernet介面。



IP過濾器

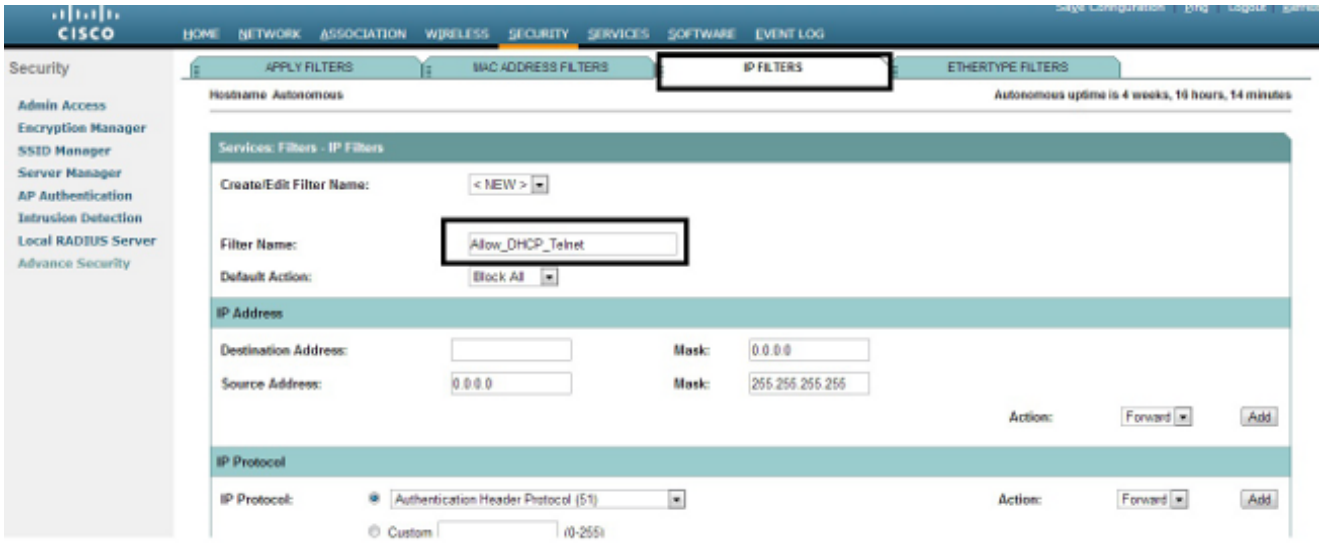
您可以使用標準型或延伸型ACL，以根據使用者端的IP位址允許或禁止使用者端裝置進入WLAN網路。

此組態範例使用延伸型ACL。延伸型ACL必須允許Telnet存取使用者端。您必須限制WLAN網路上的所有其他通訊協定。此外，客戶端使用DHCP來獲取IP地址。您必須建立一個具有以下特徵的擴展ACL:

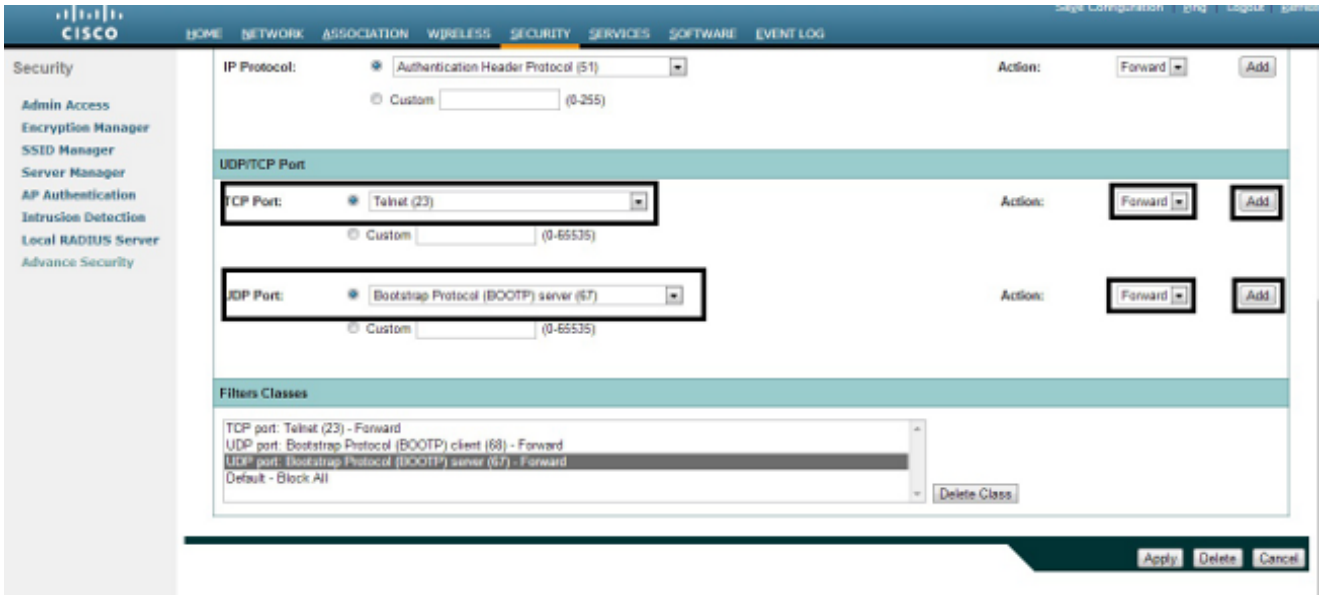
- 允許DHCP和Telnet流量
- 拒絕所有其他流量型別

完成以下步驟即可建立檔案：

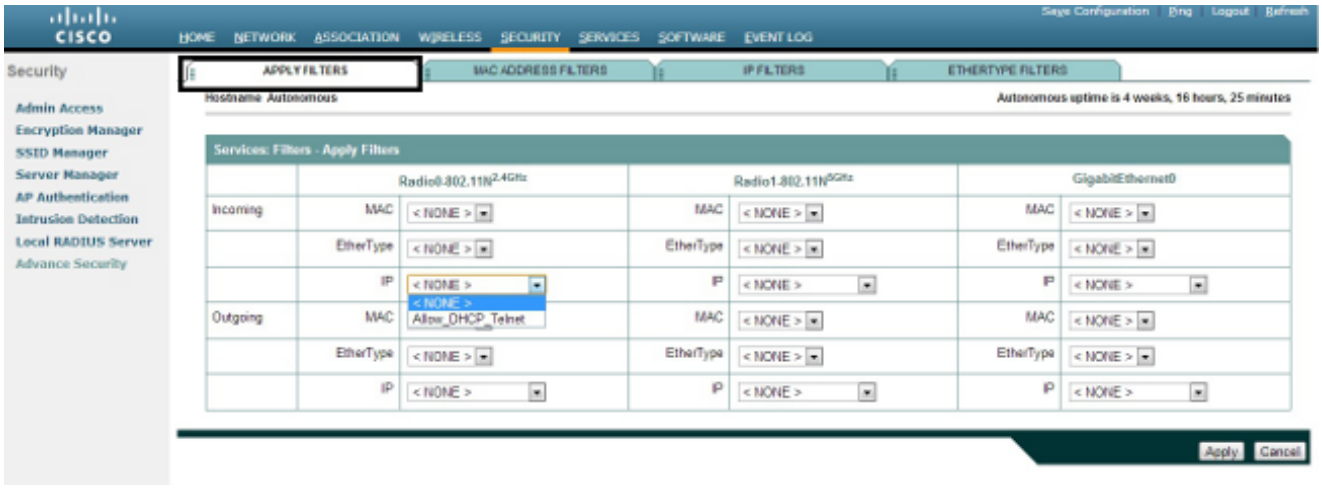
1. 為過濾器命名，並從Default Action下拉選單中選擇Block All，因為必須阻止其餘流量：



2. 從TCP Port 下拉選單中選擇Telnet，從UDP Port下拉選單中選擇BOOTP client & BOOTP server:



3. 按一下「Apply」。現在建立了IP過濾器Allow_DHCP?_Telnet，您可以將此ACL應用到傳入或傳出Radio或GigabitEthernet介面。

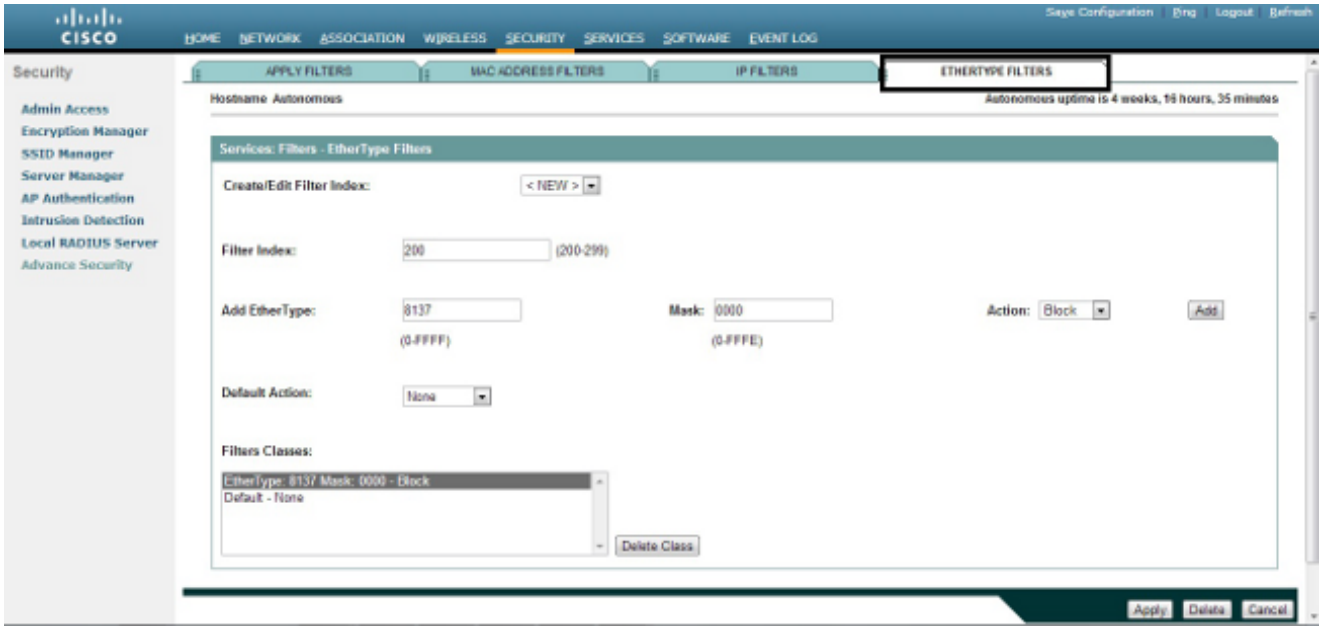


Ethertype過濾器

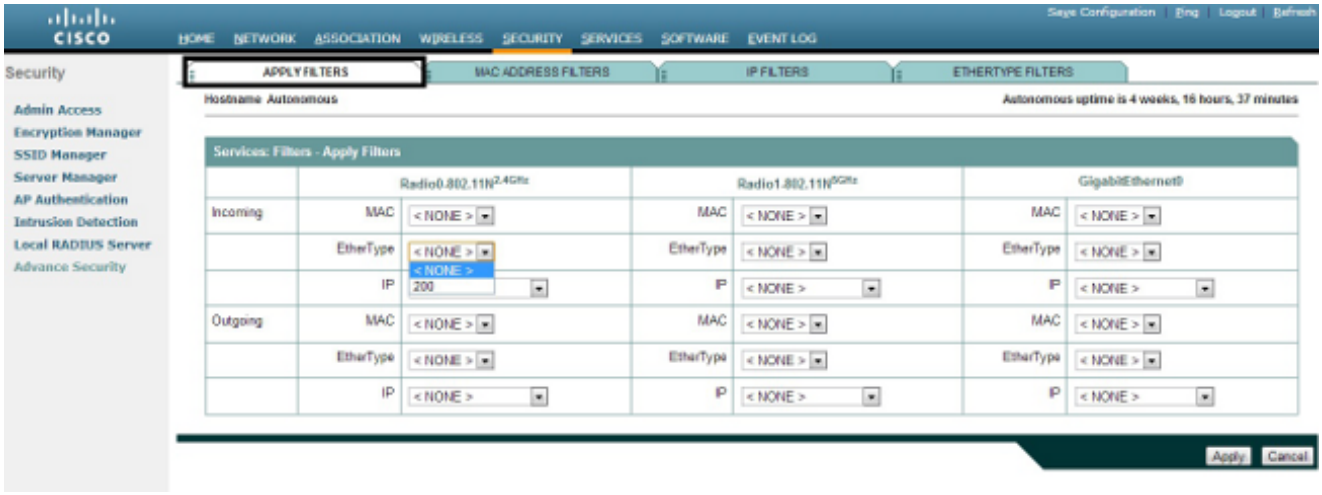
您可以使用Ethertype過濾器來阻止Cisco Aironet AP上的網際網路資料包交換(IPX)流量。這很有用的典型情況是IPX伺服器廣播會阻塞無線鏈路，這有時發生在大型企業網路中。

完成以下步驟，以設定和應用封鎖IPX流量的過濾器：

1. 按一下Ethertype Filters頁籤。
2. 在「Filter Index」欄位中，將過濾器命名為200到299之間的數字。指定的編號將為過濾器建立ACL。
3. 在Add Ethertype欄位中輸入8137。
4. 將Mask欄位中Ethertype的掩碼保留為預設值。
5. 從操作選單中選擇Block，然後按一下Add。



6. 若要從「篩選器類」清單中刪除Ethertype，請選擇它，然後按一下刪除類。重複前面的步驟，並將型別8138、00ff和00e0新增到篩選器中。現在，您可以將此ACL應用於傳入或傳出無線電或GigabitEthernet介面。



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。