# 在WAP121和WAP321存取點上為基於IPv4的存取控制清單(ACL)建立和設定規則

## 目標

訪問控制清單(ACL)是一個網路流量過濾器清單和相關操作清單，用於提高安全性。ACL包含允許或拒絕訪問網路裝置的主機。QoS功能包含區分服務(DiffServ)支援，允許將流量分類為流，並根據定義的每跳行為給予某些QoS處理。

本文說明如何在WAP121和WAP321存取點(WAP)上建立和設定基於IPv4的ACL。

## 適用裝置

·WAP121
· WAP321

## 軟體版本

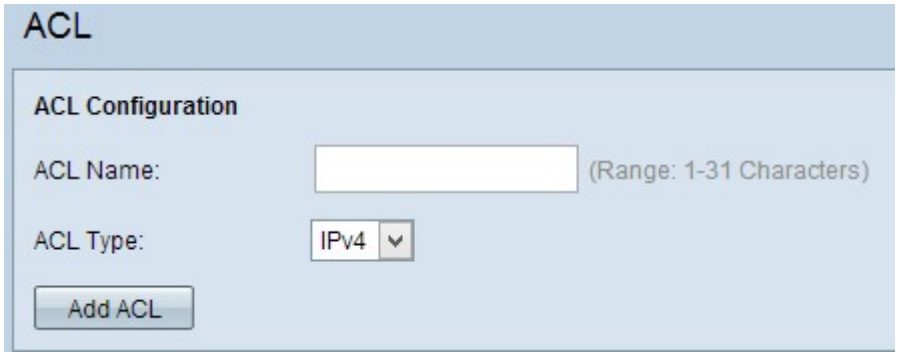
·v1.0.3.4

## 基於IPv4的ACL配置

IP ACL會對IP堆疊中第3層的流量進行分類。每個ACL是一組最多10條規則，應用於從無線客戶端傳送或由無線客戶端接收的流量。每個規則指定是否應該使用給定欄位的內容來允許或拒絕對網路的訪問。規則可以基於各種標準，並可應用於資料包中的一個或多個欄位，例如源或目標IP地址、源或目標埠或資料包中攜帶的協定。

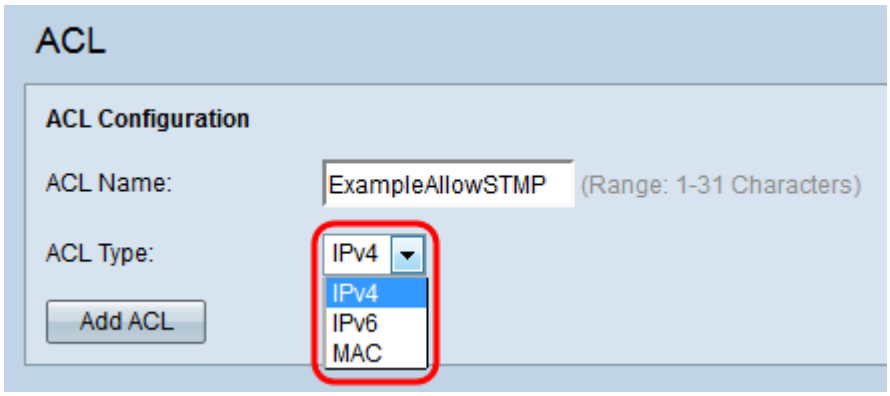
### 建立IPv4 ACL

步驟1.登入到Access Point Configuration Utility，然後選擇**Client QoS > ACL**。*ACL*頁面隨即開啟：




步驟2.在「ACL名稱」欄位中輸*入ACL的*名稱。


步驟3.從*ACL Type*下拉選單中選擇ACL的**IPv4型別。**




步驟4.按一下**Add ACL**以建立一個新的IPv4 ACL。

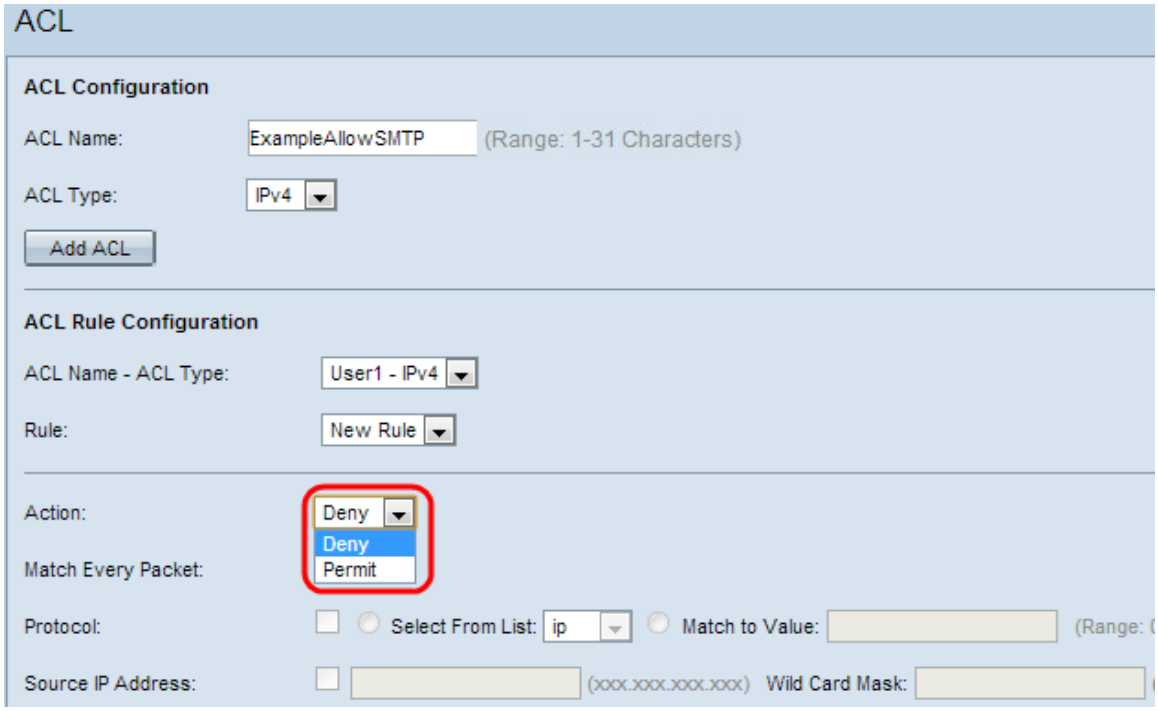

## 為IPv4 ACL配置規則

步驟1.從*ACL Name-ACL Type*下拉選單中選擇ACL，必須為其配置規則。


步驟2.如果必須為所選ACL配置新規則，請從*Rule*下拉選單中選擇**New Rule**;否則，從*Rule*下拉式清單中選擇其中一個目前規則。


**附註：**最多可為單個ACL建立10個規則。

步驟3.從Action下拉選單中選擇ACL規則的操作。

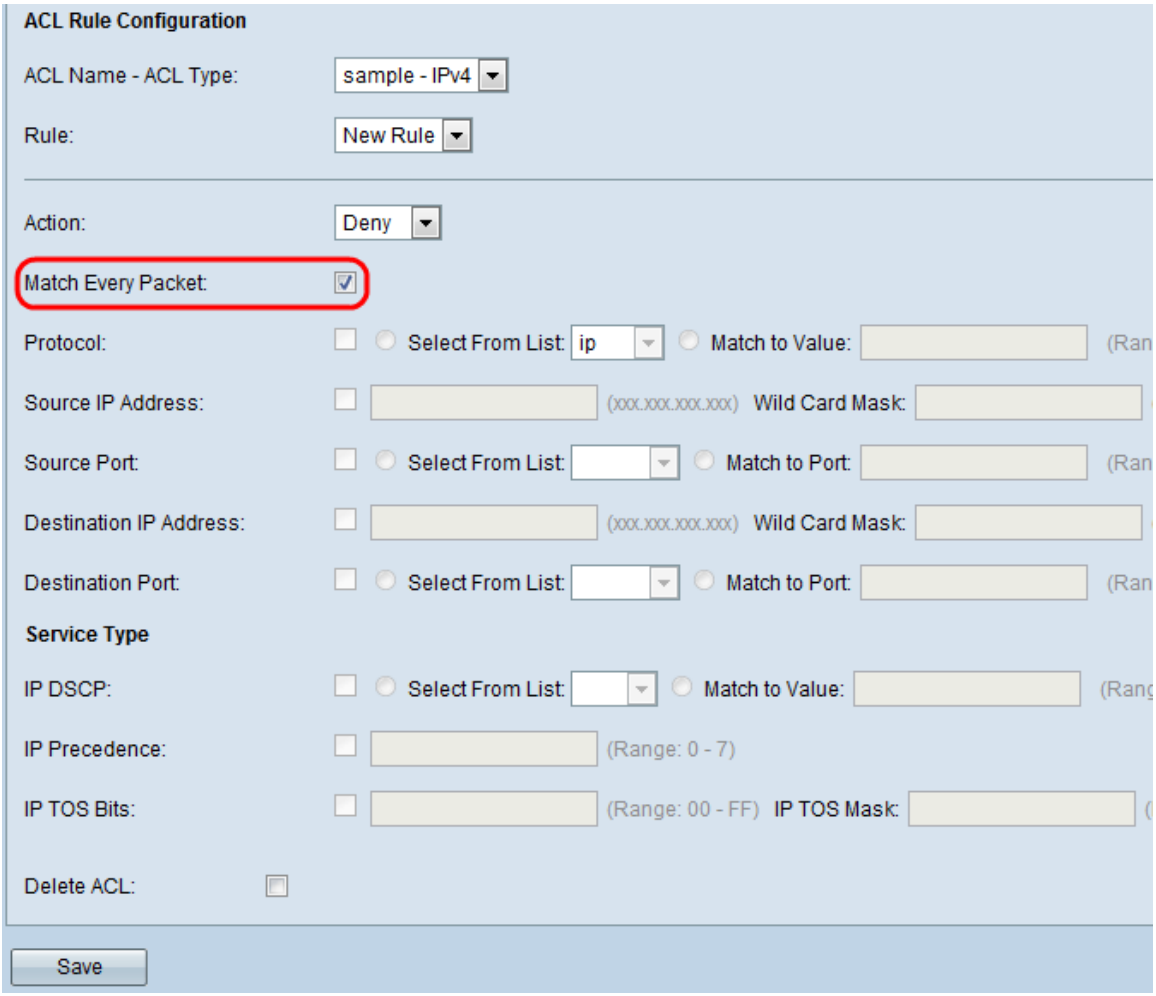



可用選項說明如下：

·拒絕 — 阻止符合規則標準的所有流量進入或退出WAP裝置。

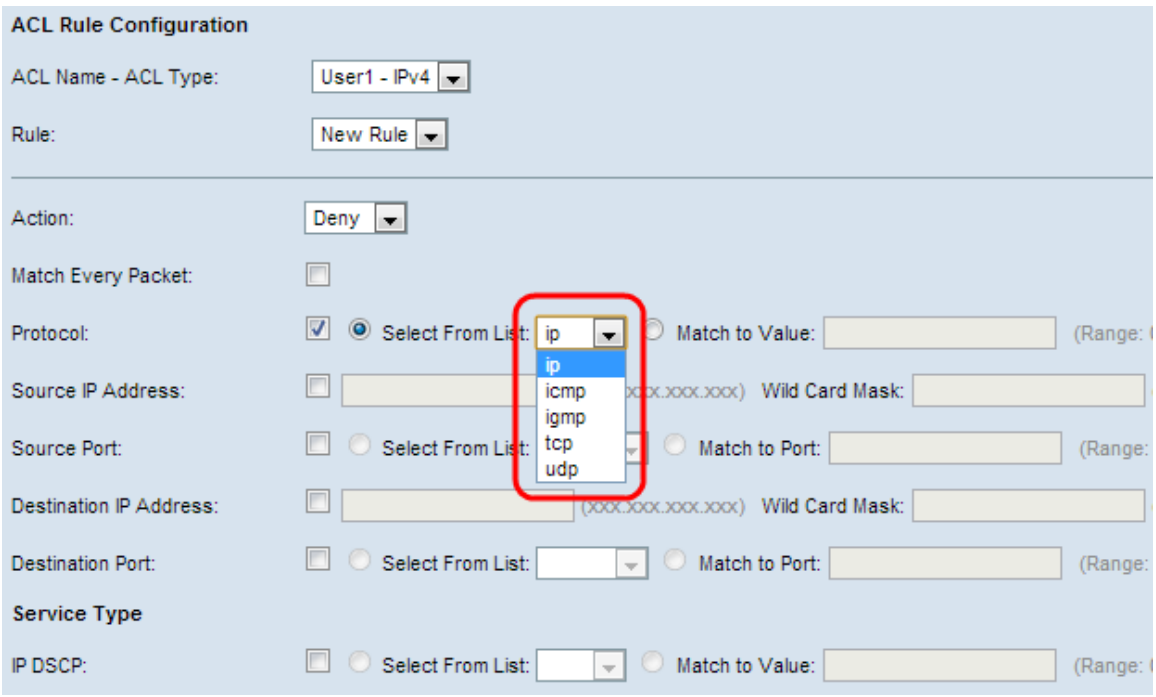
·允許 — 允許符合規則條件的所有流量進入或退出WAP裝置。

步驟4.選中*Match Every Packet*覈取方塊以匹配每個幀或資料包的規則，無論其內容如何。如果要配置特定的匹配條件，請取消選中*Match Every Packet*覈取方塊。




**時間分配器：**如果勾選「*Match Every Packet*」覈取方塊，請跳至步驟13。

步驟5.（可選）根據IPv4封包中「IP通訊協定」欄位的值，勾選L3或L4通訊協定相符條件的*通訊協定*覈取方塊。如果勾選「*Protocol*」覈取方塊，請按一下以下單選按鈕之一。



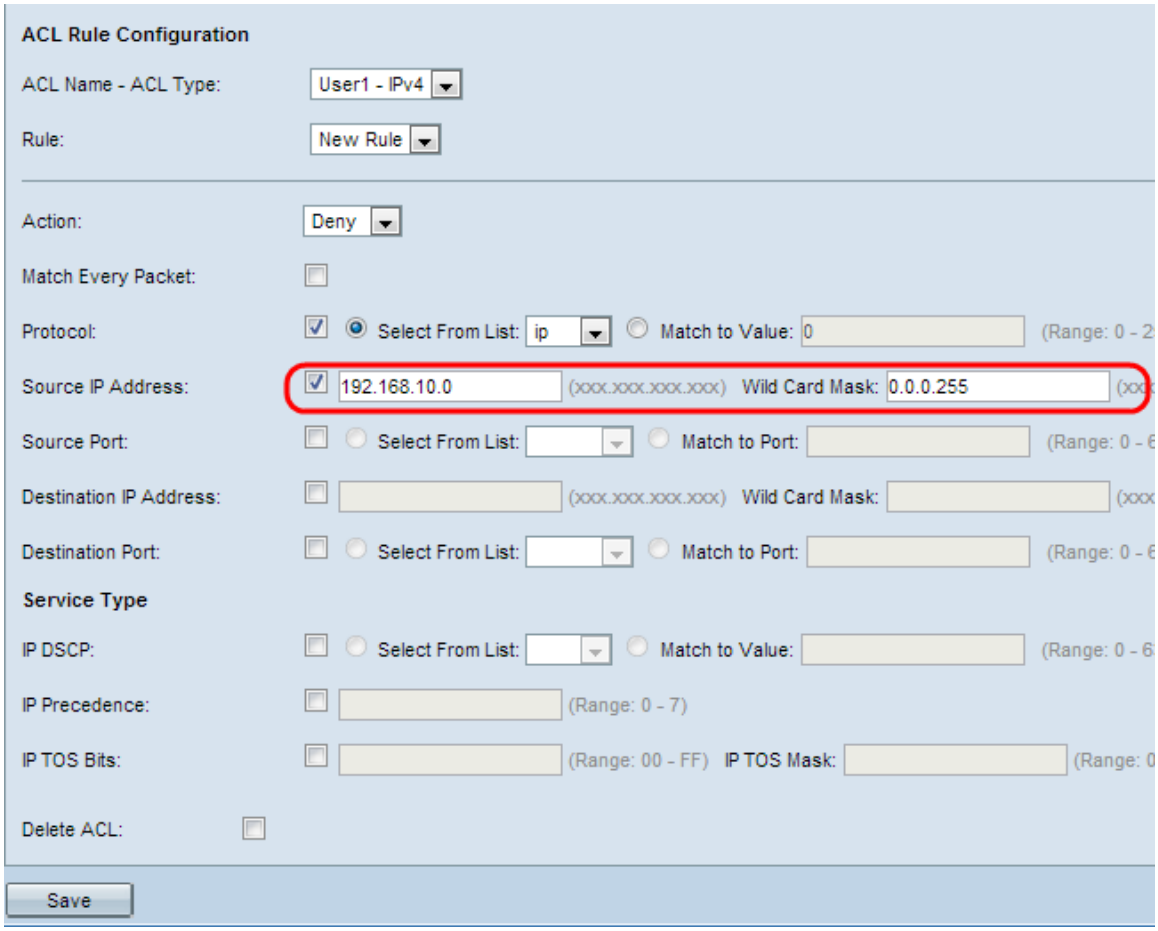

這些選項說明如下：

·從清單中選擇 — 從*從清單中選擇*一個協定。下拉選單包含ip、icmp、igmp、tcp、udp協定

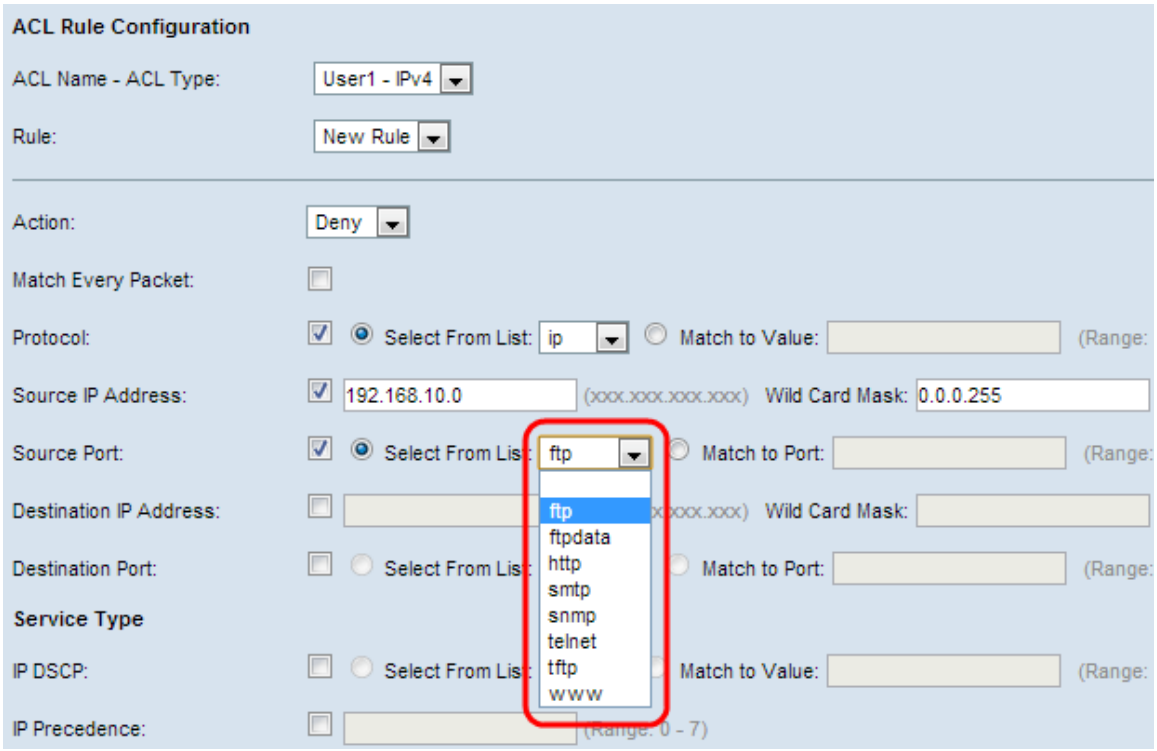
。

·與值匹配 — 適用於清單中未出現的協定。輸入從0到255的標準的IANA分配的協定ID。

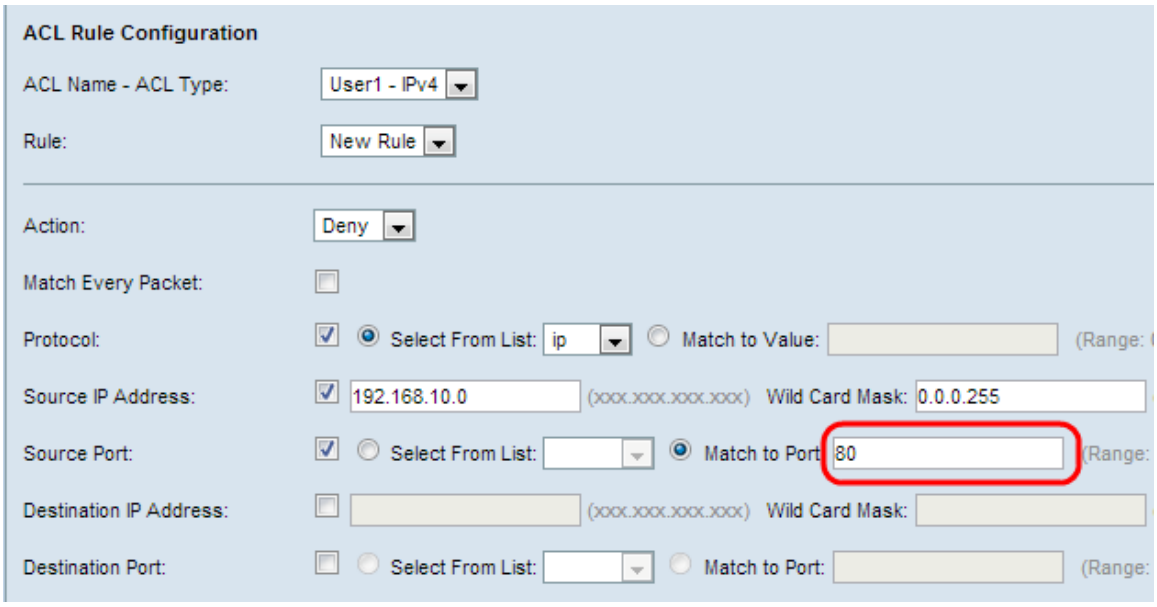
步驟6.（可選）選中*Source IP Address*覈取方塊，以在匹配條件中包含源的IP地址。在相應的欄位中輸入源的IP地址和*萬用字元掩碼*。使用萬用字元掩碼可以指定將此訪問清單應用於源IP地址的主機。




步驟7。（可選）選中**Source Port**覈取方塊以在匹配條件中包含源埠。如果勾選了「*Source Port*」覈取方塊，請按一下以下單選按鈕之一。

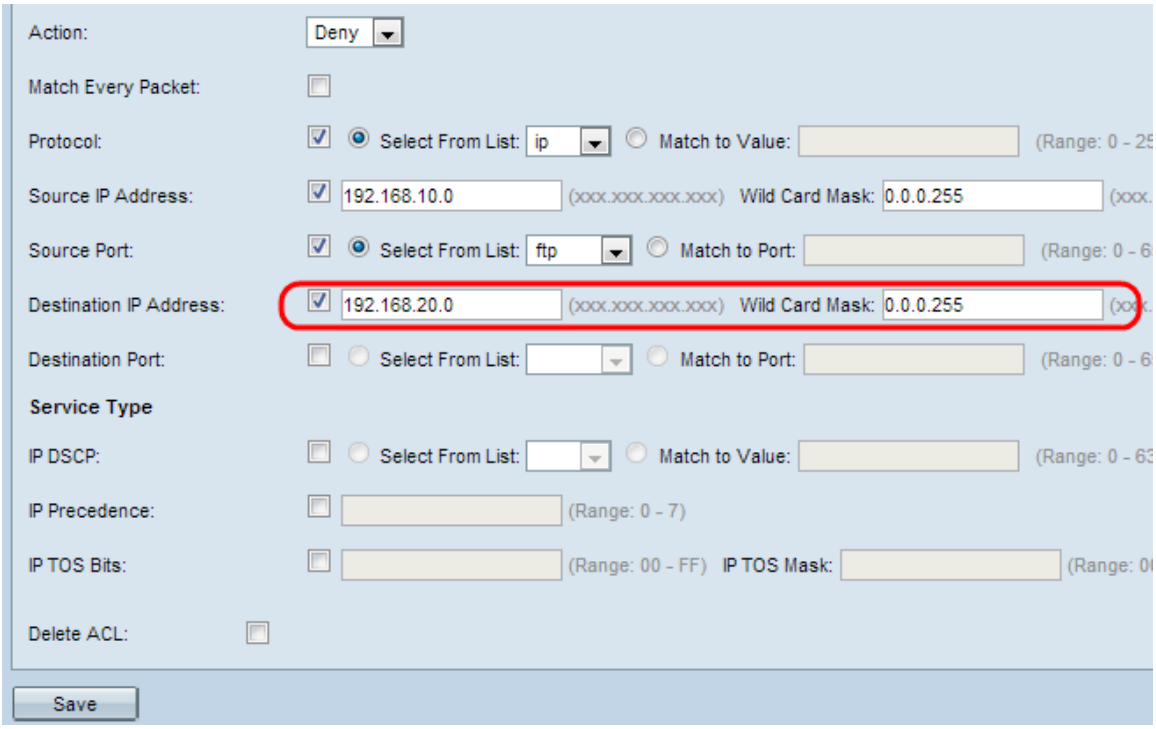



·Select From List — 從*Select From List*下拉列*表選擇*來源連線埠。下拉選單中包含ftp、ftpdata、http、smtp、snmp、telnet、tftp、www埠。

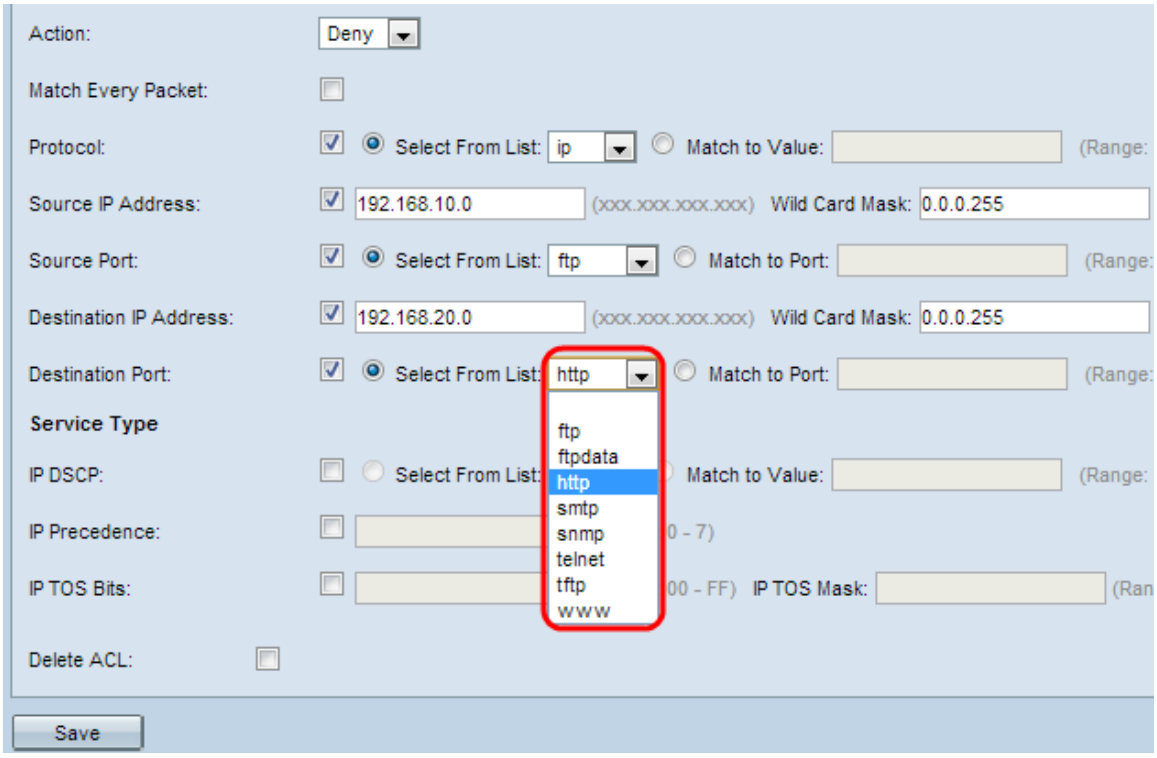



·與連線埠相符 — 適用於清單中未出現的來源連線埠。輸入範圍為0到65535的埠號。

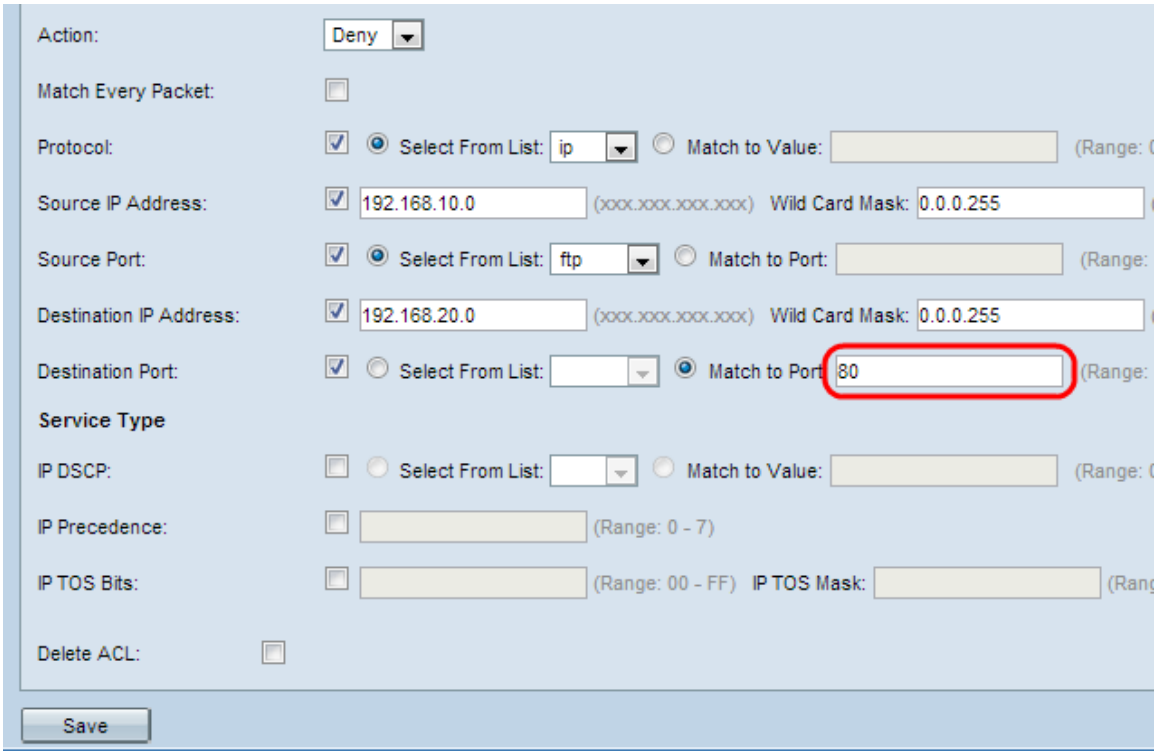
步驟8.（可選）勾選「*Destination IP Address*」覈取方塊，在匹配條件中包含目標的IP地址。在各自的欄位中輸入目的*地的IP地址*和萬用字元掩碼。使用萬用字元掩碼可以指定將此訪問清單應用於目標IP地址的主機。




步驟9.（可選）選中**Destination Port**覈取方塊以在匹配條件中包括目標埠。如果勾選「*Destination Port*」覈取方塊，請按一下以下單選按鈕之一。



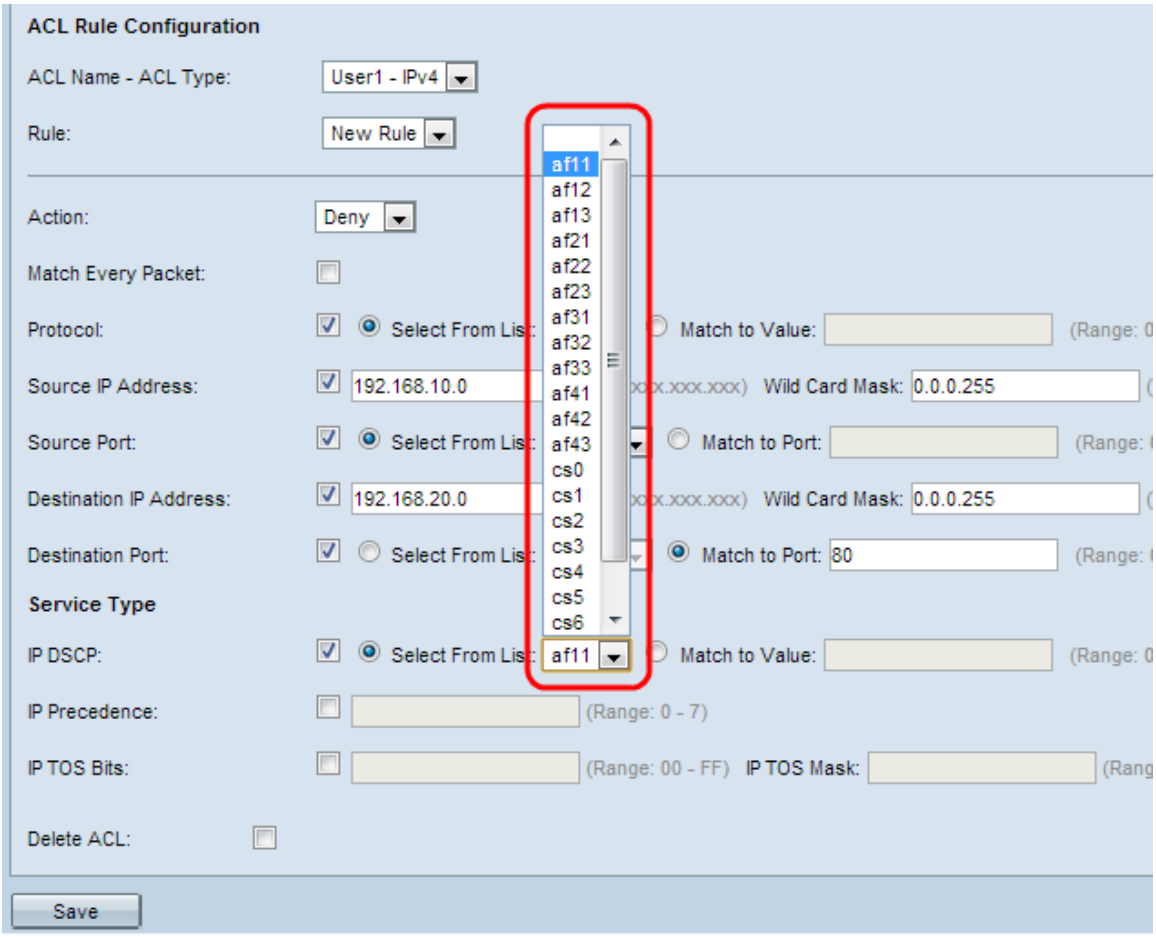

·Select From List — 從*Select From List*下拉選單*中選擇目*的地連線埠。下拉選單中包含ftp、ftpdata、http、smtp、snmp、telnet、tftp、www埠。




·與連線埠相符 — 適用於清單中未出現的目的地連線埠。在Match to Port欄位中輸入從0到65535的埠號。

**附註：**只能從*Service Type*（服務型別）區域選*擇一個*服務，並且可以為匹配條件新增這些服務。

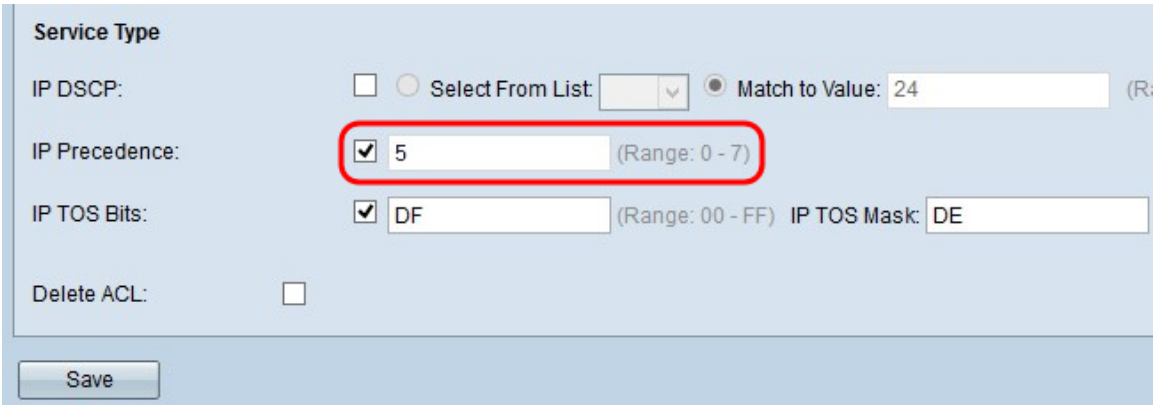
步驟10。（可選）選中*IP DSCP*覈取方塊以根據IP DSCP值匹配資料包。如果勾選「*IP DSCP*」覈取方塊，請按一下以下單選按鈕之一。DSCP用於指定幀的IP報頭上的流量優先順序。這將使用您從清單中選擇的IP DSCP值對關聯流量流的所有資料包進行分類。有關DSCP的詳細資訊，請參閱此處。



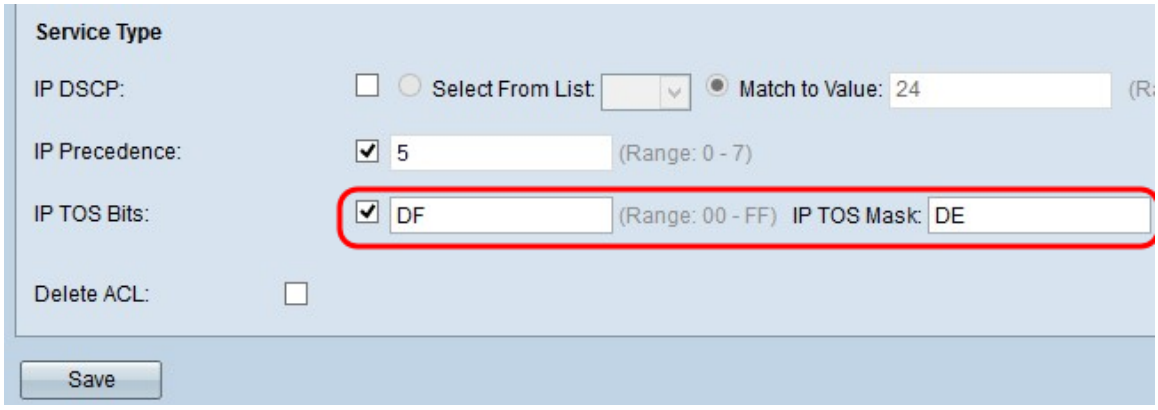

·從清單中選擇 — 從*從清單中選擇*下拉選單中選擇IP DSCP值。下拉選單具有DSCP Assured Forwarding(AS)、Class of Service(CS)或Expedited Forwarding(EF)值。

·與值匹配 — 自定義DSCP值。在Match to Value欄位中輸入範圍從0到63的DSCP值。

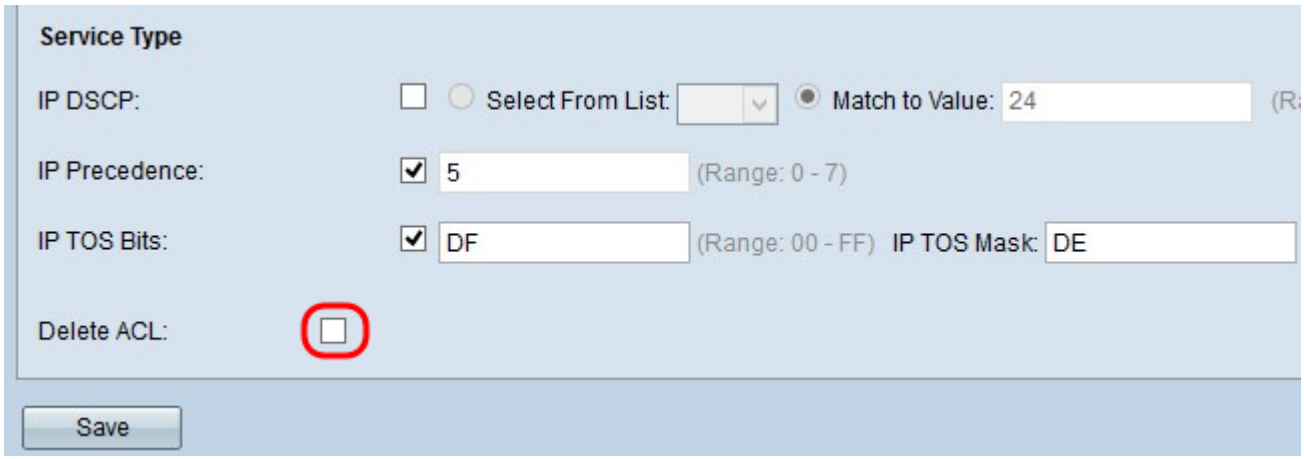
步驟11。（可選）選中*IP Precedence復*選框，在匹配條件中包含IP Precedence值。如果選中IP優先順序覈取方塊，請輸入一個範圍從0到7的IP優先順序值。有關IP優先順序的詳細資訊，請參閱此處。




步驟12.（可選）選中*IP TOS Bits*覈取方塊，以使用IP報頭中資料包的服務型別位作為匹配條件。如果選中了IP TOS Bits覈取方塊，請在相應的欄位中輸入範圍介於00-FF和00-FF的IP TOS掩碼。




步驟13。（可選）如果要刪除已配置的ACL，請選中*Delete ACL*複選框。




步驟14.按一下**Save**以儲存設定。