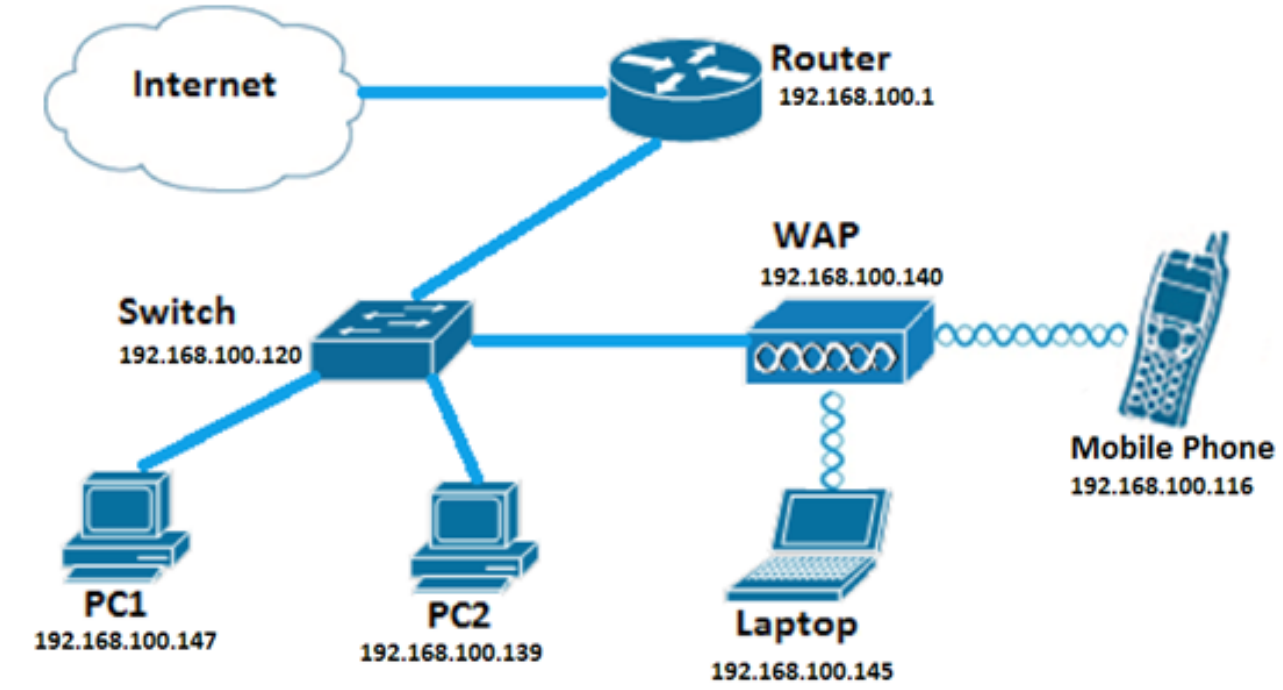
在WAP125和WAP581上配置IPv4 ACL

簡介

網際網路通訊協定第4版(IPv4)和網際網路通訊協定第6版(IPv6)存取控制清單(ACL)是一組應用於無線存取點(WAP)所接收封包的規則。 每個規則用於確定應該允許還是拒絕對網路的訪問。可以將ACL配置為檢查幀的欄位，例如源或目標IP地址、虛擬區域網(VLAN)識別符號(ID)或服務類別(CoS)。 當幀進入WAP裝置埠時，它會檢查該幀，並根據該幀的內容檢查ACL規則。如果任何規則與內容匹配，則對幀執行允許或拒絕操作。

配置IPv4 ACL通常用於授權訪問網路資源以選擇網路中的裝置。

附註：每個建立的規則的結尾都有一個隱含的deny。



附註：在此場景中，將允許來自PC2的所有流量訪問網路。來自其他主機的所有其他流量都將被拒絕。

目標

本文旨在展示如何在WAP125和WAP581存取點上設定IPv4 ACL。

適用裝置

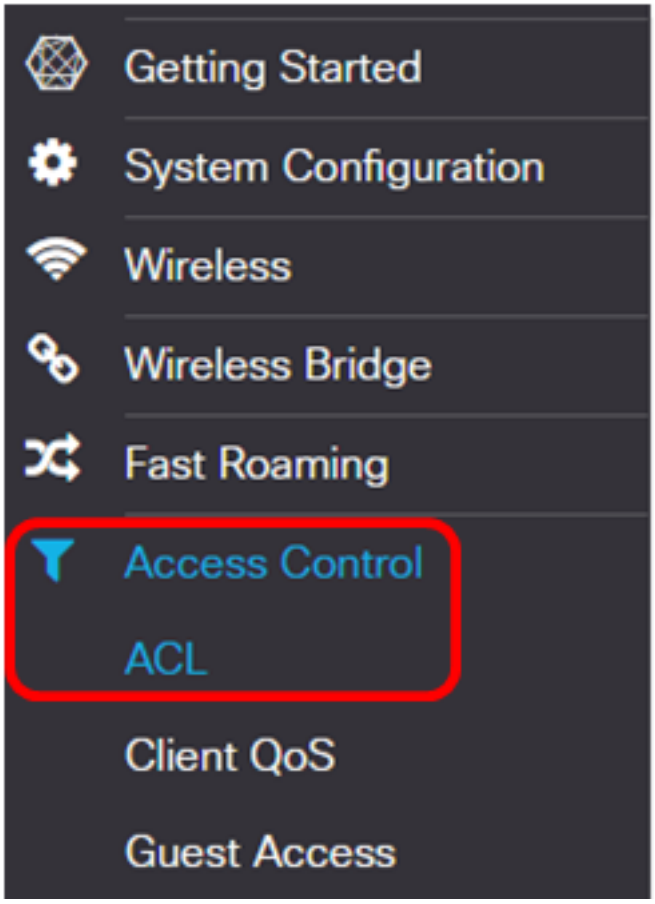
- WAP125
- WAP581

軟體版本

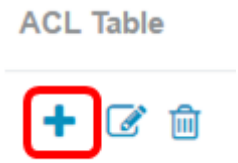
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

配置IPv4 ACL

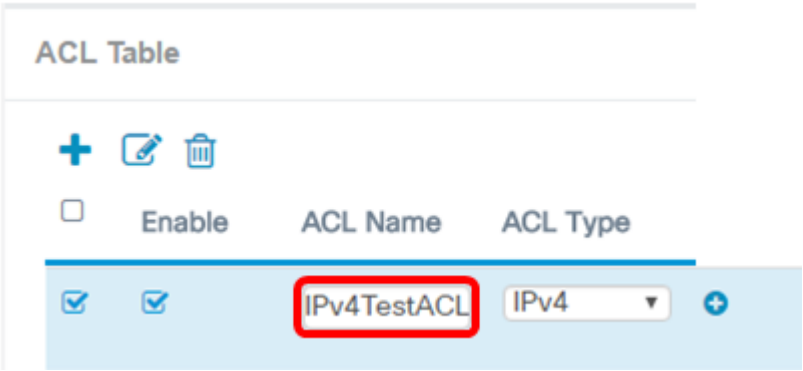
步驟1.登入到WAP的基於Web的實用程式，然後選擇**Access Control > ACL**。



步驟2.按一下 **+** 按鈕建立新的ACL。

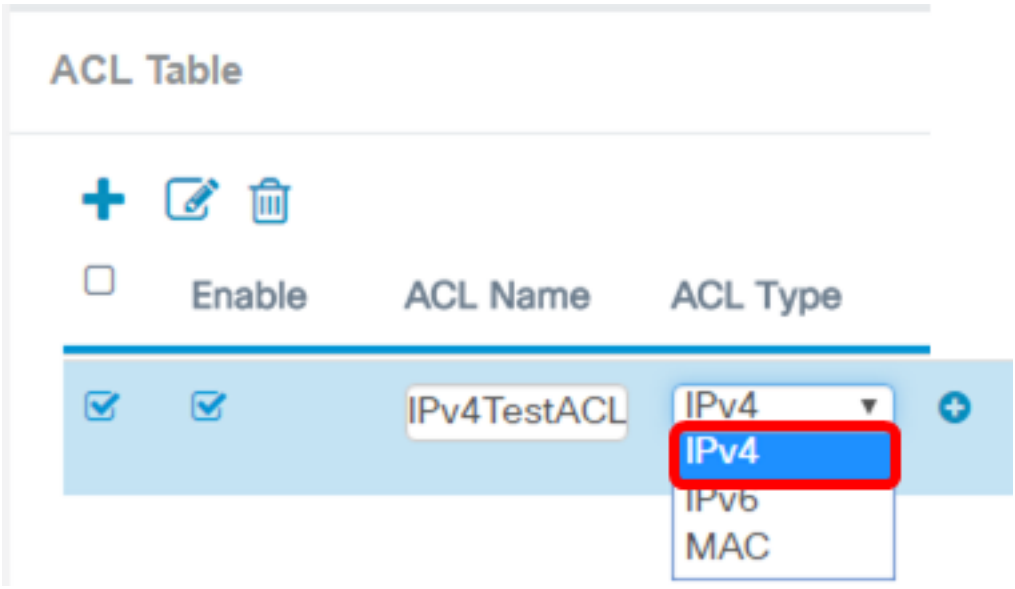


步驟3.在*ACL Name*欄位中輸入該ACL的名稱。



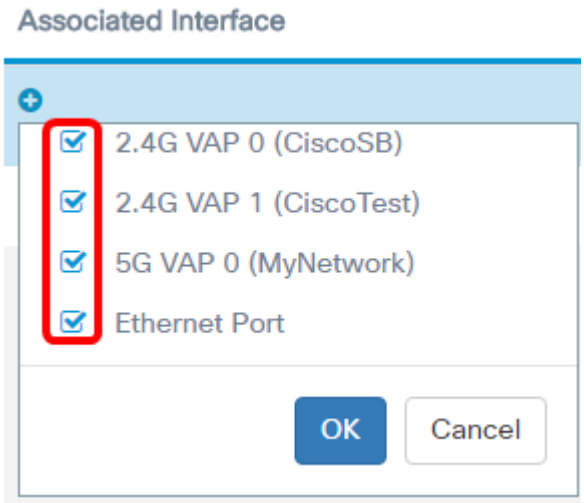
附註：在此範例中，輸入IPv4TestACL。

步驟4.從ACL Type下拉選單中選擇IPv4。



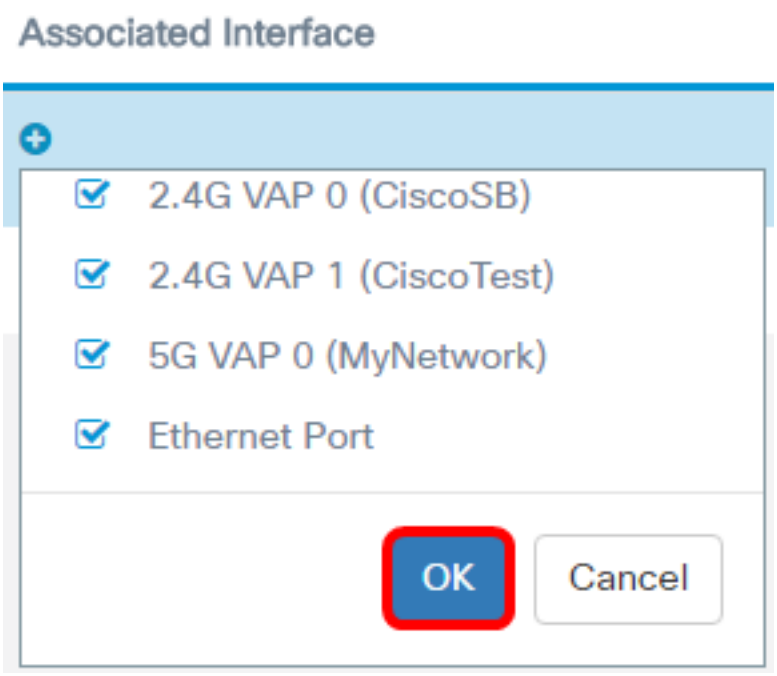
步驟5.按一下 按鈕，並從Associated Interface下拉式清單中選擇一個介面。選項包括：

- 2.4G VAP 0（SSID名稱） — 此選項將將MAC ACL應用於2.4 GHz虛擬接入點(VAP)。「SSID名稱」部分可能根據WAP上配置的SSID名稱而更改。
- 5G VAP0（SSID名稱） — 此選項將將MAC ACL應用於5 GHz VAP。
- Ethernet Port — 此選項會將MAC ACL應用於WAP的乙太網介面。



附註：可將多個介面關聯到一個ACL。但是，如果已將ACL與另一個ACL相關聯，則無法將其與該ACL相關聯。在此範例中，所有介面都與IPv4TestACL關聯。取消選中此框可將介面與ACL取消關聯。

步驟6.按一下**OK**。

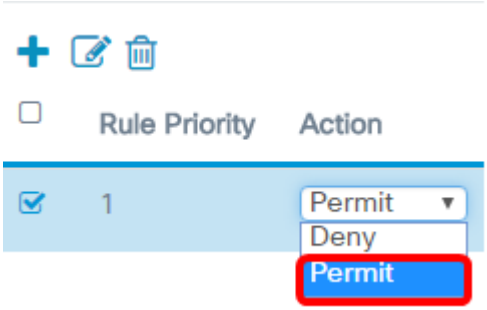


步驟7.按一下**More...**按鈕配置ACL的引數。

步驟8.按一下 ✚ 按鈕新增新規則。

步驟9.從「操作」下拉選單中選擇操作。選項包括：

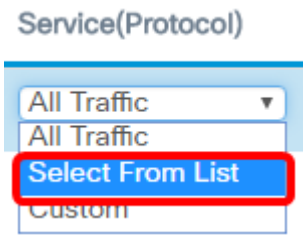
- 允許 — 此選項將允許符合ACL條件的資料包連線到網路。
- 拒絕 — 此選項將阻止符合ACL標準的資料包連線到網路。



附註：在此示例中，選擇Permit。

步驟10.從Service(Protocol)下拉選單中選擇要過濾的服務或協定。選項包括：

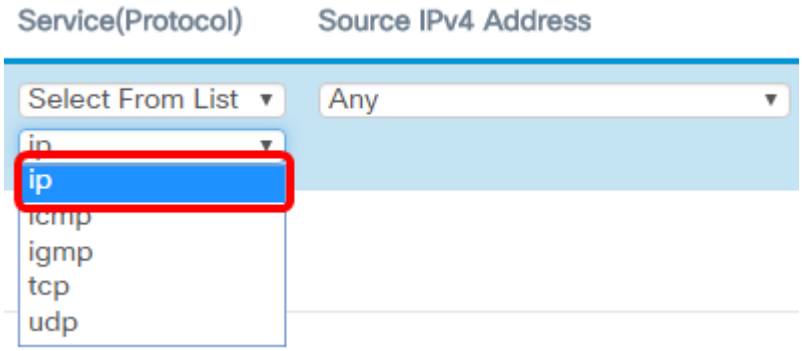
- 所有流量 — 此選項會將所有封包視為與ACL過濾器的相符。
- Select From List — 此選項可讓您選擇IP、ICMP、IGMP、TCP或UDP作為ACL的過濾器。如果選擇此選項，請繼續執行步驟11。
- 自定義 — 此選項將允許您輸入自定義協定識別符號作為資料包的過濾器。值為四位十六進位制數。範圍為0到255。



附註：在此示例中，選擇從清單中選擇。

步驟11.定義需要允許連線到網路的協定。選項包括：

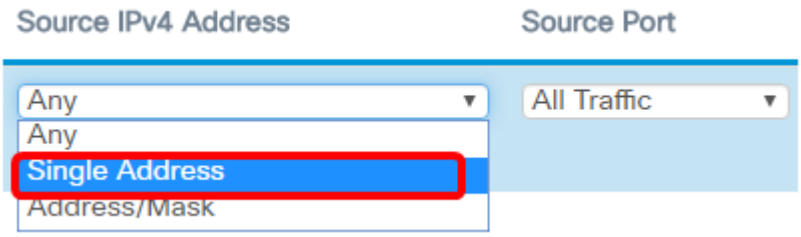
- ip — 此選項將允許接入點使用其IP地址作為過濾器來過濾訪問網路的主機。
- icmp — 此選項讓接入點過濾通過接入點進入網路的網際網路控制消息協定(ICMP)資料包。
- igmp — 此選項可讓存取點過濾透過存取點進入網路的網際網路群組管理通訊協定(IGMP)封包。
- tcp — 此選項可讓存取點過濾透過存取點進入網路的傳輸控制通訊協定(TCP)封包。
- udp — 此選項將允許接入點過濾通過接入點進入網路的使用者資料包協定(UDP)資料包。



附註：在此範例中，選擇ip。

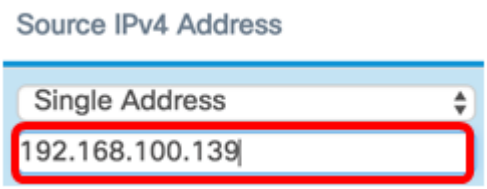
步驟12.從「源IPv4地址」下拉選單中定義源IPv4地址。選項包括：

- Any — 此選項允許WAP對來自任何IP地址的資料包應用過濾器。
- Single Address — 此選項允許WAP對來自指定IP地址的資料包應用過濾器。
- Address/Mask — 此選項可讓WAP將過濾器應用於指向IP地址和IP掩碼的資料包。



附註：在本例中，選擇了Single Address。

步驟13.輸入訪問網路時需要允許的主機的IP地址。

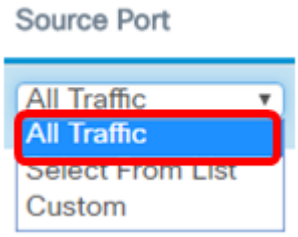


附註：在本示例中，輸入了192.168.100.139。這是PC2的IP地址。

步驟14.選擇條件的源埠。選項包括：

- 所有流量 — 此選項將允許來自源埠且符合條件的所有資料包。
- Select From List — 此選項可讓您選擇ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。
- 自定義 — 此選項將允許您輸入IANA埠號以匹配資料包報頭中標識的源埠。埠範圍從0到65535，包括以下內容：

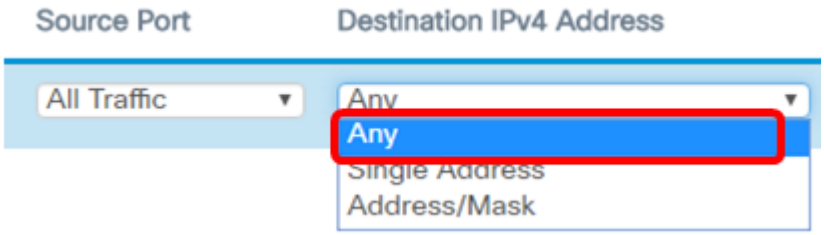
- 0到1023 — 公認埠
- 1024 — 49151 — 註冊埠
- 49152 - 65535 — 動態和/或專用埠



附註：在本例中，選擇了All Traffic。

步驟15.從Destination IPv4 Address下拉選單中選擇目的地址。選項包括：

- Any — 此選項將任何IP地址視為與ACL語句的匹配項。
- Single Address — 此選項可讓您為ACL條件輸入特定IP地址。
- 地址/掩碼 — 此選項可讓您輸入IP地址範圍或掩碼。



附註：在此示例中，選擇了Any。

步驟16.從Destination Port下拉選單中選擇目的地連線埠。選項包括：

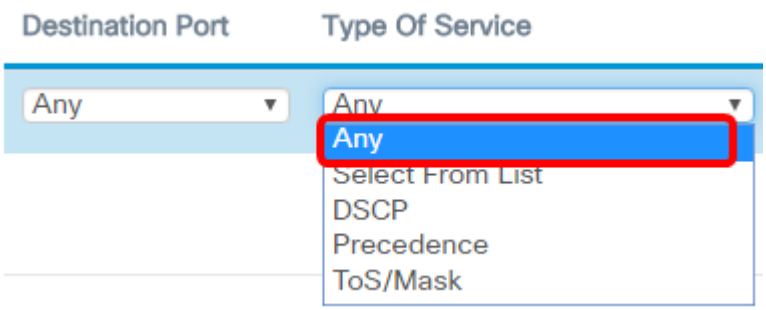
- Any — 此選項將封包的所有目的地連線埠視為與ACL中的語句相符。
- 從清單中選擇 — 此選項可讓您選擇與要匹配的目的地埠關聯的關鍵字。選項包括：ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。這些關鍵字轉換為它們對應的埠號。
- 自定義 — 此選項將允許您輸入IANA埠號以匹配資料包報頭中標識的源埠。埠範圍從0到65535，包括以下內容：

  - 0到1023 — 公認埠
  - 1024 — 49151 — 註冊埠
  - 49152 - 65535 — 動態和/或專用埠

步驟17.從Type of Service下拉選單中選擇與資料包型別匹配的服務型別。選項包括：

- Any — 此選項將任何服務視為資料包的匹配項。

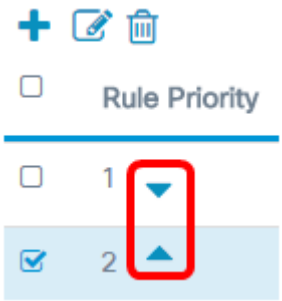
- Select From List — 此選項根據封包的區別服務代碼點(DSCP)、服務類別(CoS)或加速轉送(EF)值來比對封包。
- DSCP — 該選項根據資料包的自定義DSCP值來匹配資料包。選擇此選項時，在「DSCP值」欄位中輸入從0到63的值。
- 優先順序 — 此選項根據資料包的IP優先順序值來匹配資料包。選擇此選項後，輸入0到7之間的IP優先順序值。
- ToS/掩碼 — 此選項可讓您輸入IP ToS掩碼來標識IP Tos位值中的位位置，這些位位置用於與資料包中的IP ToS欄位進行比較。



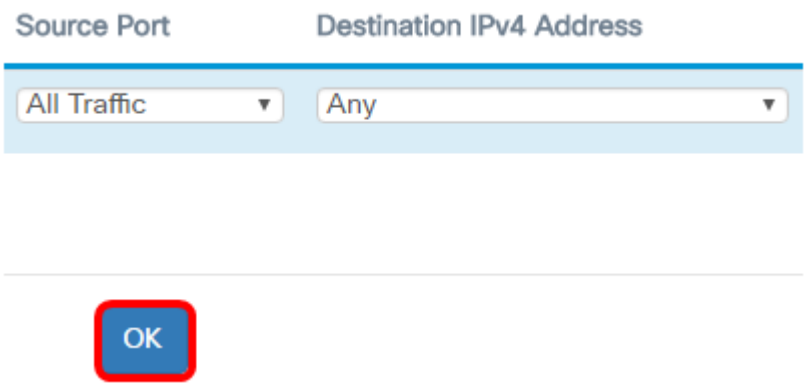
步驟18。（可選）重複步驟8到步驟17，直到ACL完成。

附註：由於建立的每個規則的結尾都有一個隱含的deny，因此無需向ACL新增拒絕規則來阻止來自網路中其他裝置的訪問。

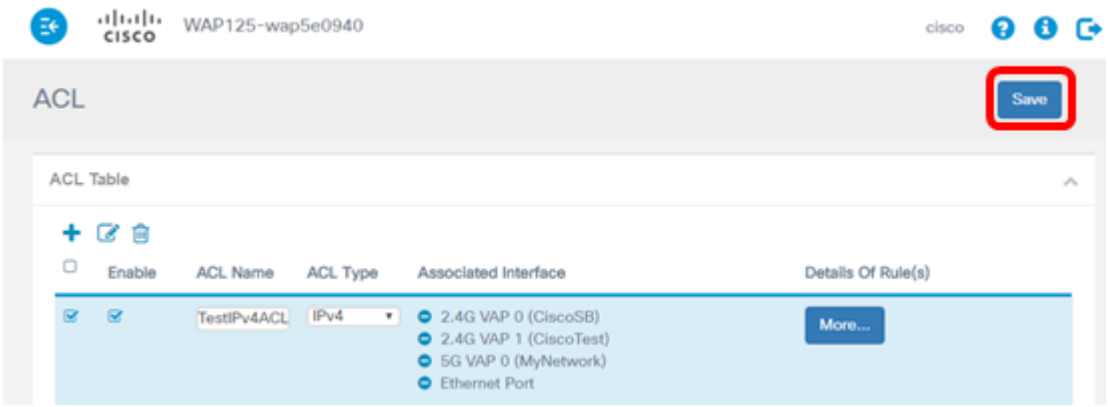
步驟19.（可選）通過按一下up和down按鈕更改ACL上條件的順序，直到它們處於正確的順序。



步驟20.按一下**OK**。



步驟21.按一下「**Save**」。



現在，您應該已經完成設定IPv4 ACL，使其在連線到WAP時僅允許一台主機訪問網路。