在200/300系列託管交換器上設定基於IPv4的存取清單

目標

訪問清單是可以應用於允許或拒絕網路上特定流量的規則，可提高網路的安全性和整體效能。

本文的目的是顯示如何在200/300系列託管交換器上設定基於IPv4的存取清單。

適用裝置

· SF/SG 200和SF/SG 300系列託管交換器

軟體版本

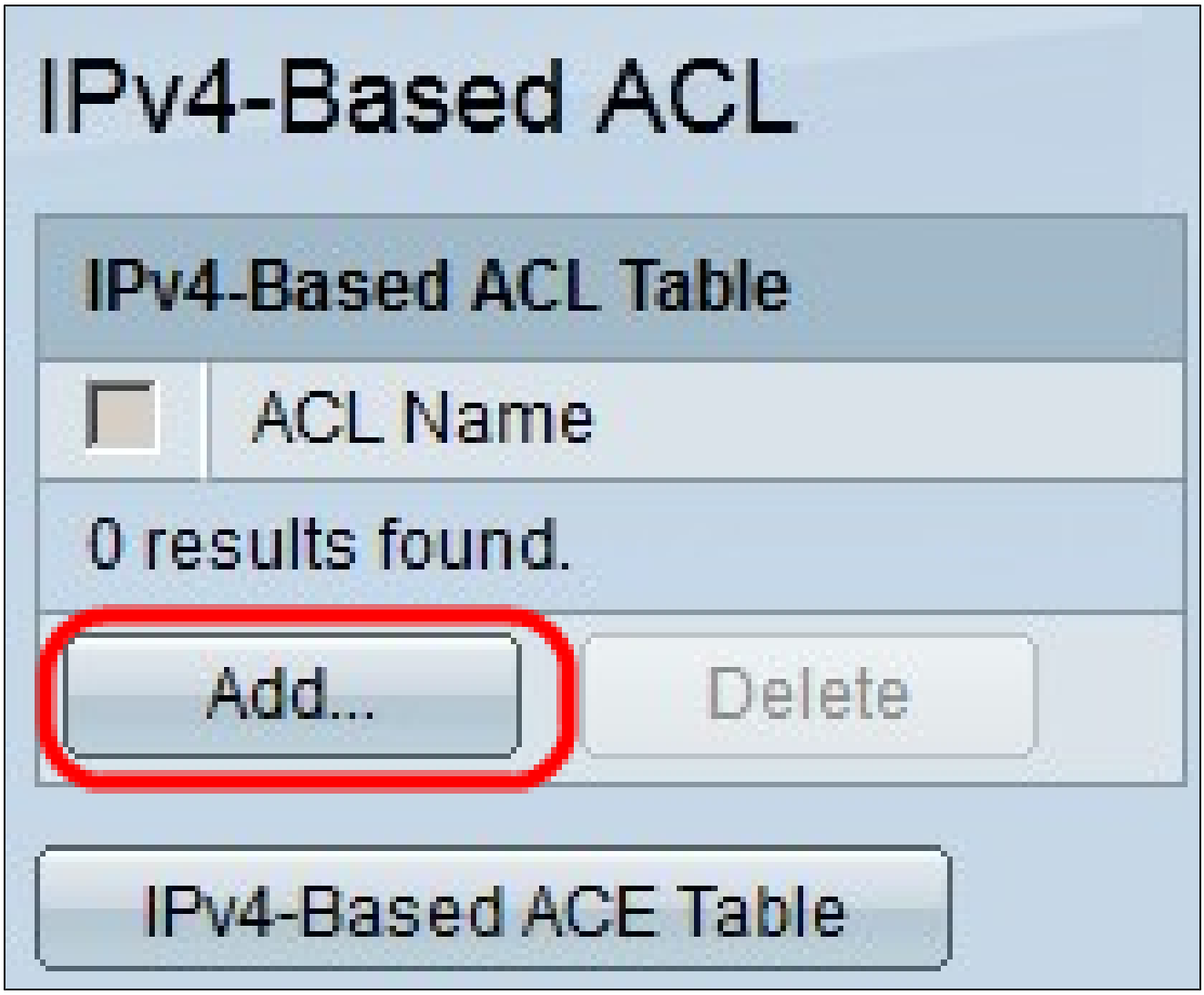
•1.3.0.62

配置基於IPv4的ACL和ACE

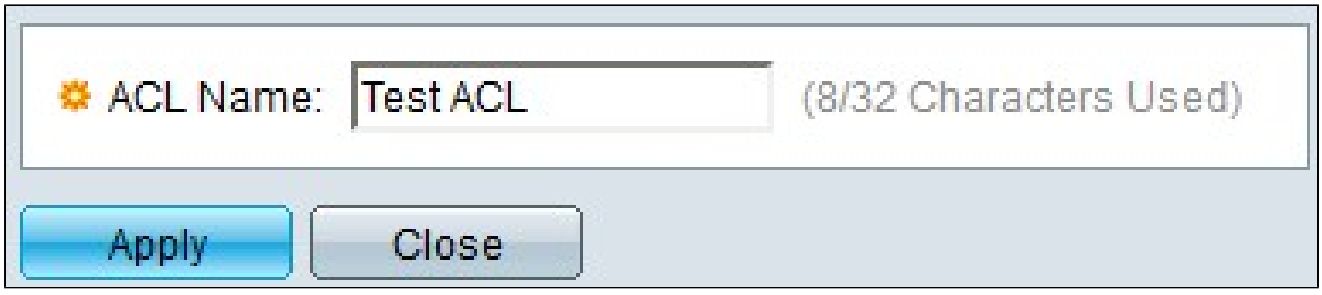
基於IPv4的ACL

步驟 1.登入Web組態公用程式，然後選擇Access Control > IPv4-Based ACL。將打開基於IPv4的ACL頁面。

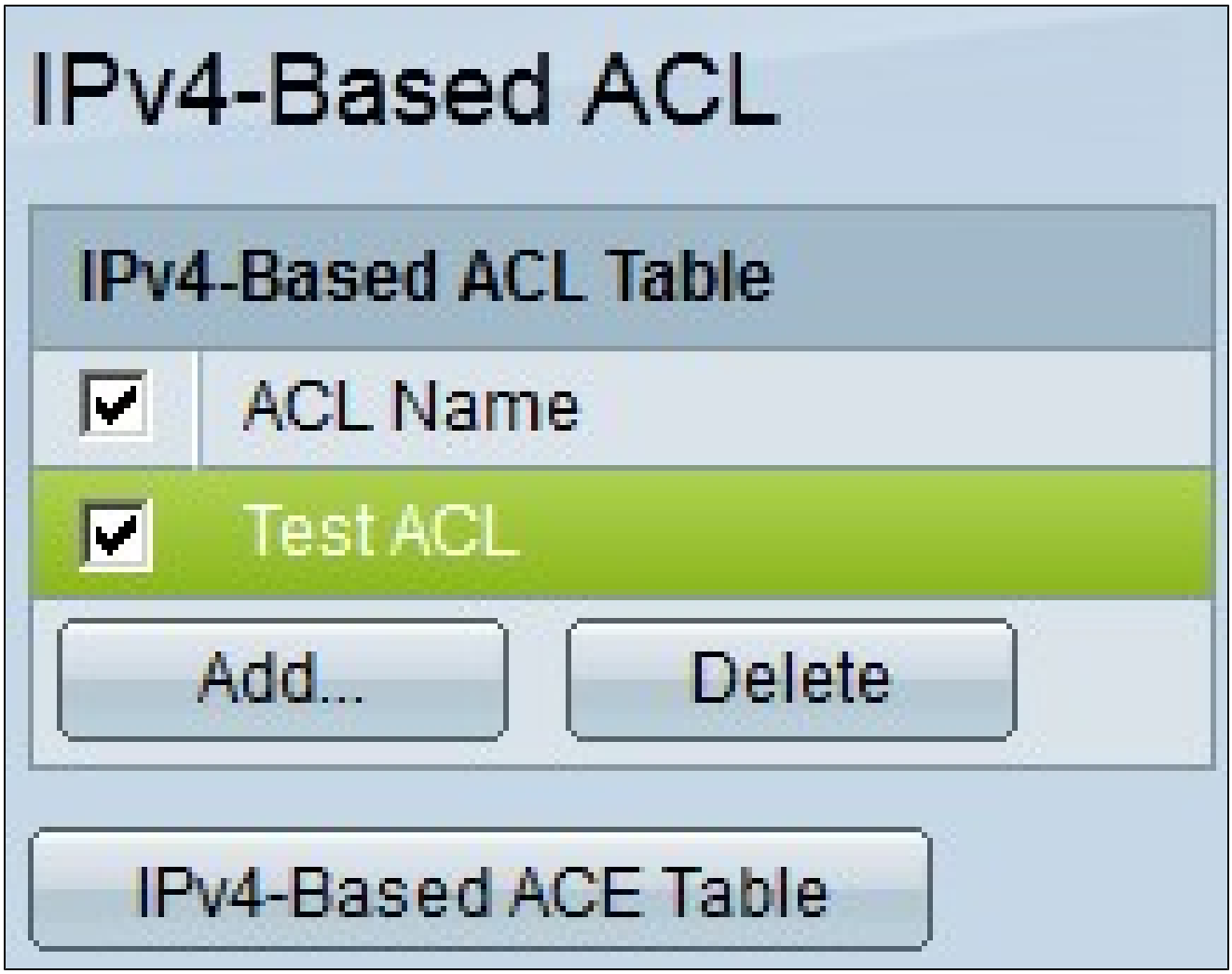
步驟 2.按一下Add以新增新訪問清單。



步驟 3.在ACL Name字段中，輸入新訪問清單的名稱。



步驟 4.按一下「Apply」以儲存存取清單。

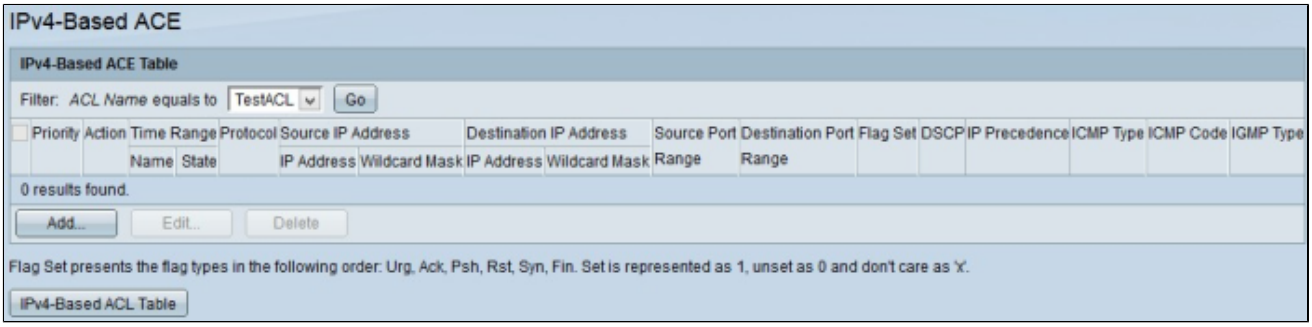


步驟5.（可選）要刪除訪問清單，請選中要刪除的訪問清單的覈取方塊，然後按一下刪除。

基於IPv4的ACE

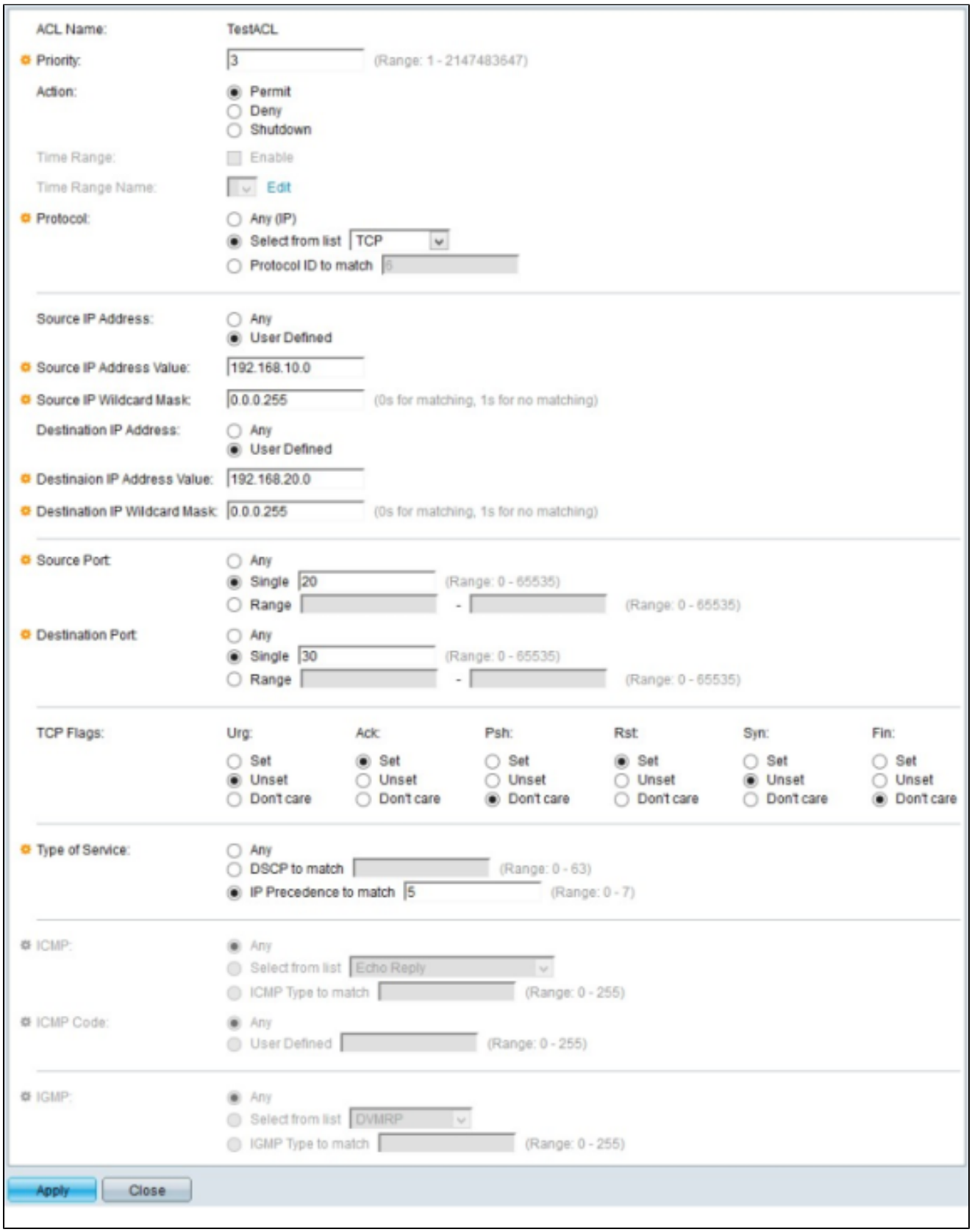
要管理ACL的ACE，需要執行後續步驟。

步驟 1.登入到Web配置實用程式並選擇訪問控制>基於IPv4的ACE。將打開基於IPv4的ACE頁面。



步驟 2.在Filter: ACL Name equals to下拉清單中，選擇要分配訪問規則的訪問清單。

步驟 3.按一下「Add」。出現Add IP-Based ACE視窗。



步驟 4.在Priority欄位中輸入ACE的優先順序。首先處理具有最高優先順序的ACE。最高優先順序為1。範圍為1到2147483647。

步驟 5.在Action欄位中，按一下希望此訪問規則執行的操作的單選按鈕。可用選項包括：

·允許 — 轉發由當前ACE過濾的資料包。

· deny — 丟棄由當前ACE過濾的資料包。

·關閉 — 丟棄由當前ACE過濾的資料包，並禁用接收資料包的埠。

步驟 6.在Protocol欄位中，按一下要新增到ACE中的協定的單選按鈕。ACE針對所有路由網路協定進行配置，以便在資料包通過路由器時過濾資料包。可用選項包括：

· Any — 選擇任何基於IPv4的ACE協定。

·從清單中選擇 — 從下拉選單中選擇所需的協定。

·要匹配的協定ID — 此選項可讓您輸入要使用的協定ID。

步驟 7.在Source IP Address欄位中，按一下其中一個可用選項作為源IP地址：

· Any — 此選項將訪問規則應用於特定網段中可用的任何IP地址。

·使用者定義 — 此選項可讓您輸入特定IP地址。

— 源IP地址值 — 在此欄位中輸入源IP地址。

— 源IP萬用字元掩碼 — 在此欄位中輸入源IP地址的萬用字元掩碼。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 8.在Destination IP Address欄位中，按一下其中一個可用選項作為目標IP地址：

· Any — 此選項將訪問規則應用於特定網段中可用的任何IP地址。

·使用者定義 — 此選項可讓您輸入應用訪問規則的特定IP地址：

— 目標IP地址值 — 在此欄位中輸入目標IP地址。

— 目標IP萬用字元掩碼 — 在此欄位中輸入目標IP地址的萬用字元掩碼。使用萬用字元掩碼可以指定應用此訪問清單的目的IP地址的主機。

步驟 9.僅當從步驟5中選擇TCP或UDP時，才會啟用Source Port欄位。按一下其中一個可用選項的單選按鈕以選擇來源連線埠：

· Any — 此選項接受任何源埠。

·單一 — 此選項可讓您輸入單個來源連線埠值。

·範圍 — 此選項可讓您輸入一組可用的來源連線埠。

步驟 10.只有從步驟5中選擇TCP或UDP時，Destination Port欄位才會啟用。按一下其中一個可用選項的單選按鈕以選擇目的地連線埠：

· Any — 此選項接受任何目的地連線埠。

·單一 — 此選項可讓您輸入單一目的地連線埠值。

·範圍 — 此選項可讓您輸入一組可用的目標埠。

步驟 11.只有從步驟5中選擇TCP時，才會啟用TCP標誌欄位。按一下每個標誌的單選按鈕之一，以選擇要觸發訪問規則的狀態：

· Urg — 此標籤將傳入資料標識為緊急。

· Ack — 此標誌用於確認成功接收資料包。

· Psh — 此標籤用於確保資料具有正確的優先順序，並在傳送端或接收端進行處理。

· Rst — 當連線接收到錯誤的資料段時，使用此標誌。

· Syn — 此標誌用於TCP通訊。

· Fin — 當通訊或資料傳輸完成時使用此標誌。

步驟 12.在「Type of Service」欄位中，按一下其中一個可用單選按鈕，為IP封包選擇服務型別：

· Any — 此選項選擇任何型別的服務。

· DSCP to match — 選擇此選項可將區別服務代碼點(DSCP)作為服務型別實施。DSCP是一種對網路流量進行分類和管理的方法。輸入要應用於訪問規則的DSCP值。

· IP優先順序匹配 — 當前網路使用此型別的服務來提供正確的QoS（服務品質）。輸入要應用於訪問規則的值。

步驟 13.只有您在步驟5中選擇ICMP時，才會啟用ICMP（網際網路控制訊息通訊協定）欄位。ICMP用於在服務不可用時傳送錯誤消息或測試連線。按一下其中一個可用單選按鈕過濾ICMP消息型別：

· Any — 可以是任何錯誤消息或查詢消息。

·從清單中選擇 — 從下拉選單中選擇任何允許的控制消息。

·要匹配的ICMP型別 — 此選項可讓您輸入要過濾的ICMP型別的數量。

步驟 14.只有從步驟5中選擇ICMP時，ICMP Code欄位才會啟用。ICMP代碼用於提供關於控制消息的更具體的資訊。按一下其中一個可用選項：

· Any — 可以是與控制消息匹配的任何值。

·使用者定義 — 輸入您要過濾的ICMP代碼。

步驟 15.只有從步驟5中選擇IGMP時，才會啟用IGMP（Internet組管理協定）欄位。IGMP管理網段上IP組播組中的主機成員資格。點選可用的單選按鈕以過濾IGMP消息型別：

· Any — 此選項接受所有IGMP消息型別。

·從清單中選擇 — 從下拉選單中選擇一個可用選項以進行篩選：

- DVMRP — 它使用反向路徑泛洪技術，該技術通過除資料包到達的介面以外的每個介面將收到的資料包的副本傳送出去。

— 主機查詢 — 它定期在每個連線的網路上傳送常規主機查詢消息以獲取資訊

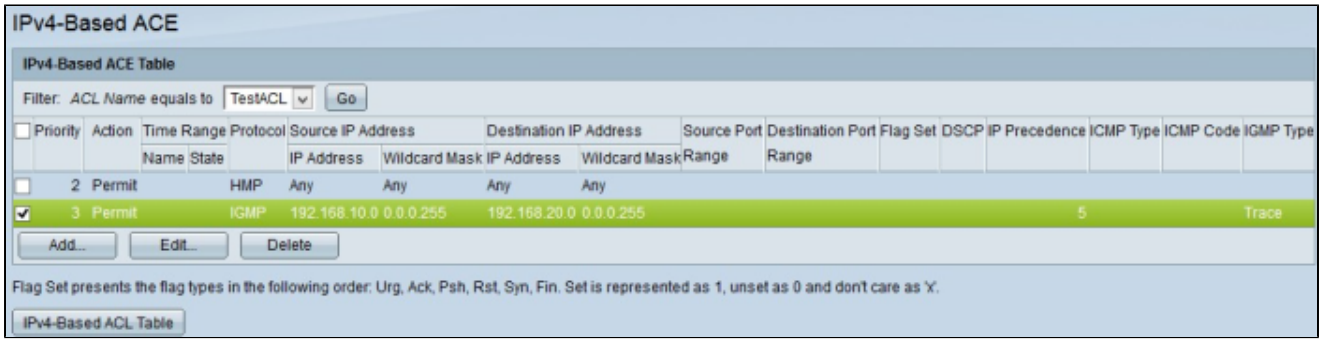
- Host-Reply — 它回複查詢。

- PIM — 本地和遠端組播路由器之間使用它來將組播流量從組播伺服器定向到許多組播客戶端。

— 跟蹤 — 它提供加入和退出IGMP組播組的資訊。

· IGMP匹配型別 — 此選項可讓您輸入要過濾的IGMP型別的數量。

步驟 16.按一下「Apply」以儲存組態。



步驟17.（可選）要編輯當前訪問規則，請選中要編輯的訪問規則的覈取方塊，然後按一下編輯。

步驟18.（可選）要刪除當前訪問規則，請選中要刪除的訪問規則的覈取方塊，然後按一下刪除。

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）。