200/300系列託管交換器上的存取設定檔組態

目標

訪問配置檔案充當交換機的另一安全層。 訪問配置檔案最多可包含128條規則以提高安全性。每個規則都包含一個操作和一個標準。如果訪問方法與管理方法不匹配，則阻止使用者訪問裝置。

本文說明如何配置配置檔案以訪問200/300系列託管交換機。

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

訪問配置檔案配置

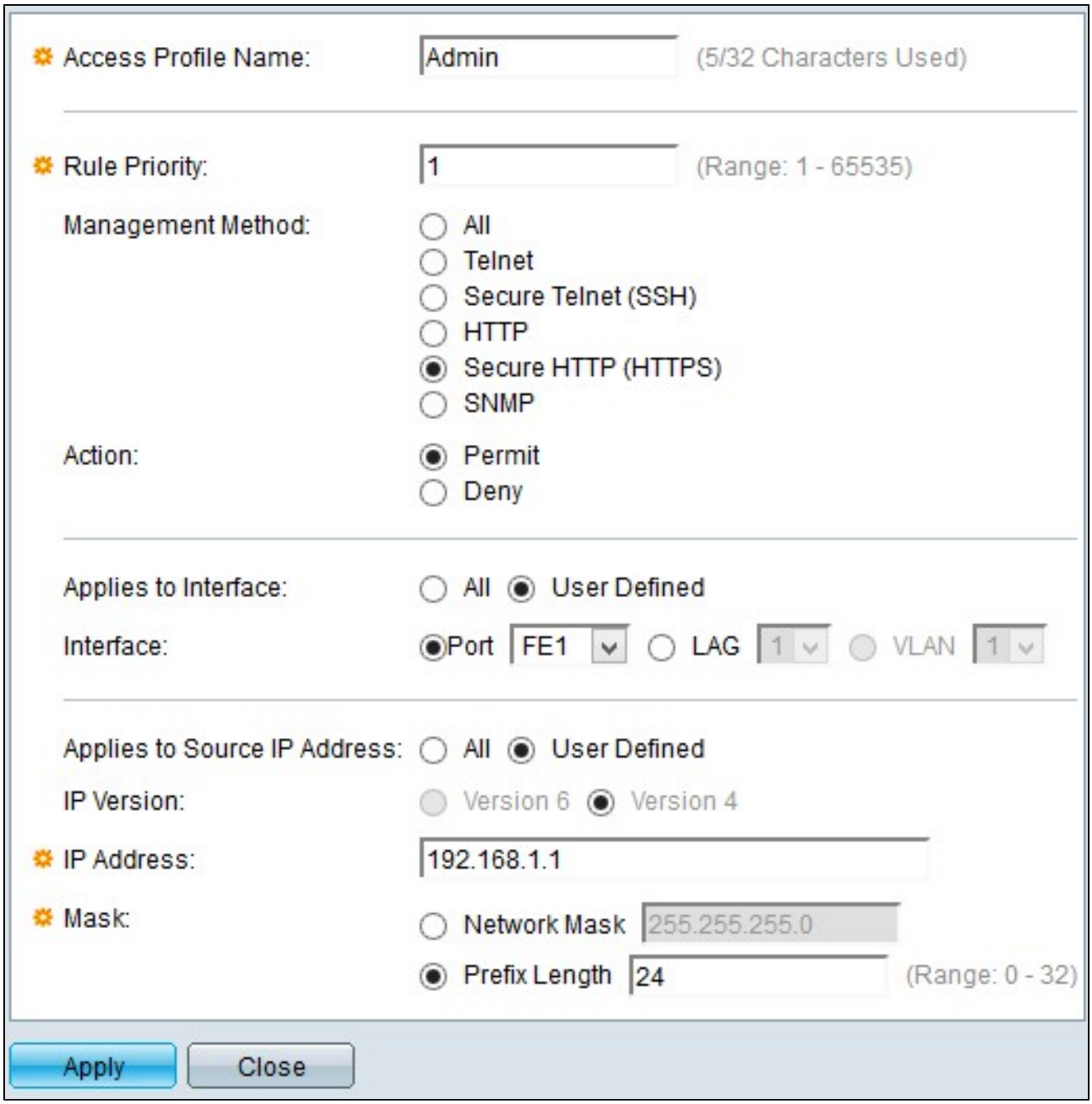
步驟 1.登入到Web配置實用程式，然後選擇Security > Mgmt Access Method > Access Profiles。Access Profiles 頁面隨即開啟：

步驟 2.從Active Access Profile下拉選單中選擇所需的訪問配置檔案。

步驟 3.按一下Apply以更改當前活動的訪問配置檔案。

新增訪問配置檔案

步驟 1.在Access Profile Table中按一下Add。此時會顯示Add Access Profile 視窗：



步驟 2.在訪問配置檔名稱欄位中輸入訪問配置檔案的名稱。

步驟 3.在Rule Priority欄位中輸入規則的優先順序。規則優先順序將資料包與規則相匹配。首先檢查優先順序較低的規則。如果資料包與規則匹配，則執行所需的操作。

步驟 4.在Management Method欄位中點選與所需管理方法對應的單選按鈕。使用者使用的訪問方法必須與要執行的操作的管理方法匹配。可能的方法有：

·全部 — 所有管理方法都分配給訪問配置檔案。

· Telnet — 分配給規則的Telnet管理方法。只有使用Telnet會議訪問配置檔案方法的使用者才

能訪問該裝置。

·安全Telnet(SSH) — 為配置檔案分配SSH管理方法。只有具有Telnet會議訪問配置檔案的使用者才能訪問該裝置。

· HTTP — 將HTTP管理方法分配給配置檔案。只有使用HTTP會議訪問配置檔案方法的使用者才能訪問該裝置。

·安全HTTP(SSL) — 向配置檔案分配HTTPS管理方法。只有使用HTTPS會議訪問配置檔案方法的使用者才能訪問該裝置。

· SNMP — 將SNMP管理方法分配給配置檔案。只有使用SNMP會議訪問配置檔案方法的使用者才能訪問該裝置。

步驟 5.從Action下拉選單中選擇要附加到規則的操作。可能的操作值為：

· Permit — 允許訪問交換機。

·拒絕 — 拒絕存取交換器。

步驟 6.點選與「應用於介面」(Apply to Interface)欄位中的所需介面型別對應的單選按鈕，以定義訪問配置檔案的介面。這兩個選項是：

·所有 — 包括所有介面，例如埠、VLAN和LAG。

注意:LAG是組合多個物理鏈路以提供更多頻寬的邏輯鏈路。

·使用者定義 — 僅應用於使用者所需的介面。

— 埠 — 從埠下拉選單中選擇要為其定義訪問配置檔案的埠。

- LAG — 從LAG下拉選單中選擇LAG，從LAG下拉選單中為其定義訪問配置檔案。

- VLAN — 從VLAN下拉選單中選擇要從VLAN下拉選單中選擇其訪問配置檔案的VLAN。

步驟 7.點選Source IP Address單選按鈕以啟用介面源IP地址。有兩個可能的值：

·所有 — 包括所有IP地址。

·使用者定義 — 僅應用於使用者所需的IP地址。

— 第6版 — 用於IP第6版(IPv6)地址。

— 版本4 — 用於IP版本4(IPv4)地址。

步驟 8.如果您在步驟7中選擇了User Defined，請在IP Address欄位中輸入裝置的IP地址。

步驟 9.按一下其中一個選項的Mask欄位中的單選按鈕以定義網路掩碼。可用選項包括：

·網路掩碼 — 輸入以點分十進位制格式與IP地址對應的子網掩碼。

·字首長度 — 輸入與IP地址對應的子網掩碼字首長度。

步驟 10.按一下「Apply」。

步驟11。（可選）要刪除訪問配置檔案，請選中要刪除的訪問配置檔案的覈取方塊，然後點選刪除。

步驟12。（可選）按一下Profile Rules Table以轉到「Profile Rules」頁。

注意：有關配置檔案規則的詳細資訊，請參閱200/300系列託管交換機上的訪問配置檔案規則配置一文。

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）。