

200/300系列託管交換器上的存取設定檔規則組態

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，則使用者將被阻止，無法訪問交換機。

本文說明如何在200/300系列託管交換器上設定設定設定檔規則。

適用裝置

- SF/SG 200和SF/SG 300系列託管交換器

軟體版本

- v1.2.7.76

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 > Profile Rules。此時將打開「概要文件規則」頁：

Access Profile Name	Priority	Management Method	Action	Interface	Source IP Address	Prefix Length
<input checked="" type="checkbox"/> Guest	1	Secure HTTP (SSL)	Permit	FE3	192.168.10.0	24
<input type="checkbox"/> Console Only	1	All	Deny			

步驟 2.選中Filter覈取方塊以顯示在Access Profile 頁中建立的訪問配置檔名稱。

步驟 3. 從 Access Profile Name equals to 下拉選單中選擇所需的訪問配置檔案。

步驟 4. 按一下 Go 以顯示所需的訪問配置檔案。

步驟 5. (可選) 若要開始新搜尋，請按一下 Clear Filter。

新增配置檔案規則

步驟 1. 選中與要新增規則的訪問配置檔案對應的覈取方塊。

步驟 2. 按一下「Add」。此時會顯示 Add Profile Rule 視窗。

Access Profile Name:	<input type="text" value="Guest"/>
<hr/>	
☛ Rule Priority:	<input type="text" value="2"/> (Range: 1 - 65535)
Management Method:	<input type="radio"/> All <input type="radio"/> Telnet <input checked="" type="radio"/> Secure Telnet (SSH) <input type="radio"/> HTTP <input type="radio"/> Secure HTTP (HTTPS) <input type="radio"/> SNMP
Action:	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
<hr/>	
Applies to Interface:	<input type="radio"/> All <input checked="" type="radio"/> User Defined
Interface:	<input checked="" type="radio"/> Port <input type="text" value="FE4"/> <input type="radio"/> LAG <input type="text" value="1"/> <input type="radio"/> VLAN <input type="text" value="1"/>
<hr/>	
Applies to Source IP Address:	<input type="radio"/> All <input checked="" type="radio"/> User Defined
IP Version:	<input type="radio"/> Version 6 <input checked="" type="radio"/> Version 4
☛ IP Address:	<input type="text" value="192.168.20.0"/>
☛ Mask:	<input type="radio"/> Network Mask <input type="text" value=""/> <input checked="" type="radio"/> Prefix Length <input type="text" value="24"/> (Range: 0 - 32)
<hr/>	
<input type="button" value="Apply"/>	<input type="button" value="Close"/>

步驟3. (可選) 要將配置檔案規則新增到不同的配置檔名稱，請從Access Profile Name下拉選單中選擇不同的配置檔名稱。

步驟 4. 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 5. 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。

·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。只有具有安全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。僅具有HTTPS會議訪問配置檔案方法的使用者可以訪問裝置。
- SNMP — 將SNMP管理方法分配給配置檔案。僅具有SNMP會議訪問配置檔案方法的使用者可以訪問裝置。

步驟 6.從「操作」單選按鈕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 7.點選與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。

- 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 8.按一下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。

— 版本6 — 用於IP版本6地址。

— 版本4 — 用於IP版本4地址。

步驟 9.如果您選擇步驟7中的User Defined，請在IP Address欄位中輸入裝置的IP地址。

步驟 10.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 11.按一下「Apply」。

 Access Profile Name equals to Guest Go Clear Filter'. Below the filter is a table with columns: Access Profile Name, Priority, Management Method, Action, Interface, Source IP Address, and Prefix Length. The table contains three rows: 1. Guest (Priority 1, Secure HTTP (SSL), Permit, FE3, 192.168.10.0, 24) with an unchecked checkbox. 2. Guest (Priority 2, Secure Telnet (SSH), Permit, FE4, 192.168.20.0, 24) with a checked checkbox. 3. Console Only (Priority 1, All, Deny) with an unchecked checkbox. Below the table are buttons for 'Add...', 'Edit...', and 'Delete'. At the bottom of the section is a button for 'Access Profiles Table'."/>

<input type="checkbox"/>	Access Profile Name	Priority	Management Method	Action	Interface	Source IP Address	Prefix Length
<input type="checkbox"/>	Guest	1	Secure HTTP (SSL)	Permit	FE3	192.168.10.0	24
<input checked="" type="checkbox"/>	Guest	2	Secure Telnet (SSH)	Permit	FE4	192.168.20.0	24
<input type="checkbox"/>	Console Only	1	All	Deny			

步驟12. (可選) 要編輯當前訪問配置檔案，請選中要編輯的訪問配置檔名稱的覈取方塊，然後按一下編輯。

步驟13. (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。

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）。