

將存取控制清單(ACL)繫結到200/300系列託管交換器上的介面

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可通過三種方式中的一種來定義：通過MAC地址、IPv4地址或IPv6地址。當ACL繫結到介面時，到達該介面的資料包將與ACL進行匹配，並會允許或丟棄該資料包。但是，每個介面只能繫結一個ACL。

本檔案將說明如何將ACL繫結到200和300系列託管交換器上的介面。

適用裝置

- SF/SG 200和SF/SG300系列託管交換器

軟體版本

- 1.3.0.62

將訪問控制清單繫結到介面

步驟 1.登入到Web配置實用程式，然後選擇Access Control > ACL Binding。此時將開啟「ACL繫結」頁：

ACL Binding

A port can be bound with either a [policy](#) or an ACL, but not both.

The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL. To change the default action of an ACL to forward those packets by configuring Permit Any on the desired port.

ACL Binding Table

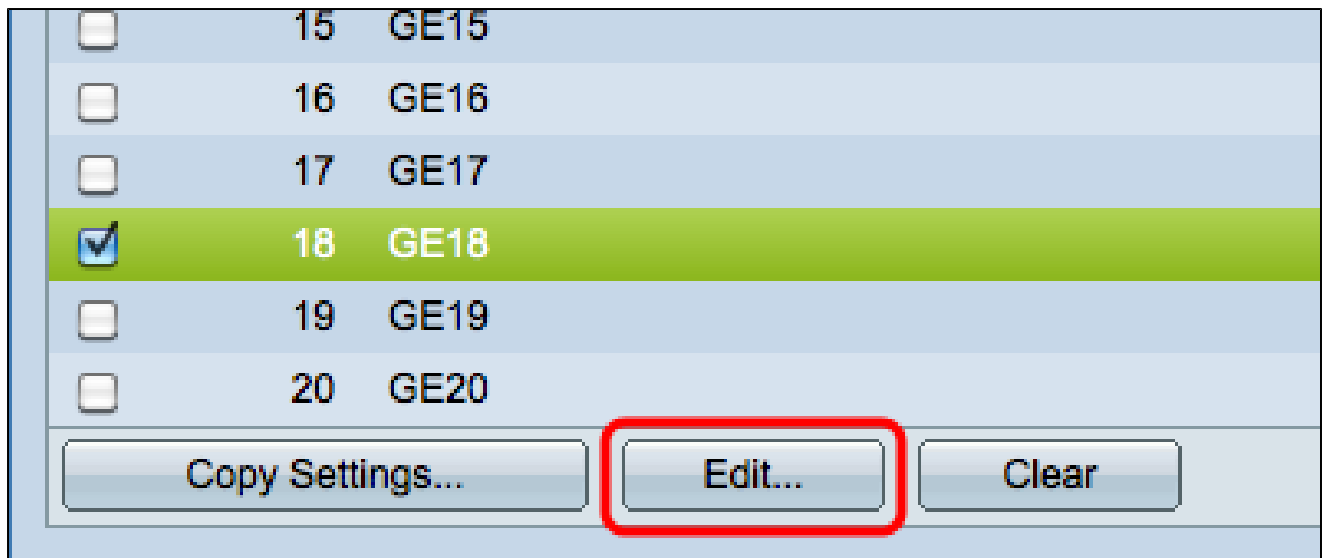
Filter: *Interface Type* equals to Port ▾ Go

<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Permit Any
<input type="checkbox"/>	1	GE1				
<input type="checkbox"/>	2	GE2				
<input type="checkbox"/>	3	GE3				
<input type="checkbox"/>	4	GE4				
<input type="checkbox"/>	5	GE5				
<input type="checkbox"/>	6	GE6				
<input type="checkbox"/>	7	GE7				

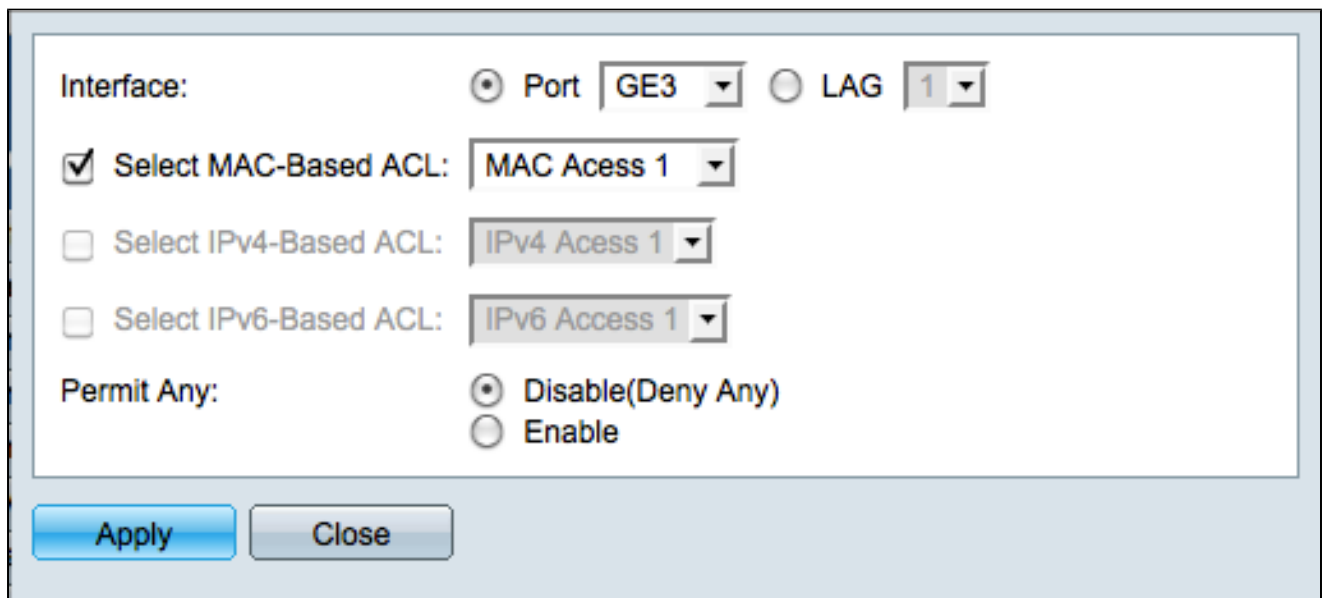
步驟 2. 從 Interface Type 下拉選單中選擇一個介面，然後按一下 Go。

- 埠 — 交換機上的單個物理埠。
- LAG — 一組用於提高鏈路可靠性的埠。

步驟 3. 選中所需埠/LAG 的覈取方塊，然後點選 Edit。



系統將顯示Edit ACL Binding視窗。



步驟 4.選中要繫結到選定介面的ACL型別的覈取方塊，然後從下拉選單中選擇ACL。

- 基於MAC的ACL — 根據幀報頭的第2層欄位過濾流量。
- 基於IPv4的ACL — 根據IPv4封包過濾流量。
- 基於IPv6的ACL — 根據IPv6資料包過濾流量。

註：只有在此格式中存在可用的ACL時，才會突出顯示任何ACL選項的覈取方塊。

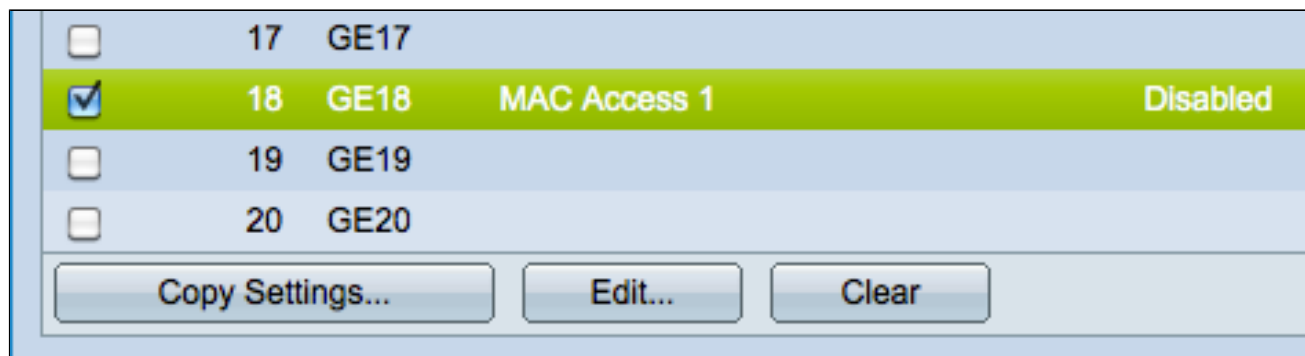
步驟 5.選中Permit Any欄位中的相應單選按鈕，定義如何處理與所選ACL不匹配的資料包。

·停用(Deny Any) — 如果封包與ACL不相符，便會將其捨棄 (拒絕)。

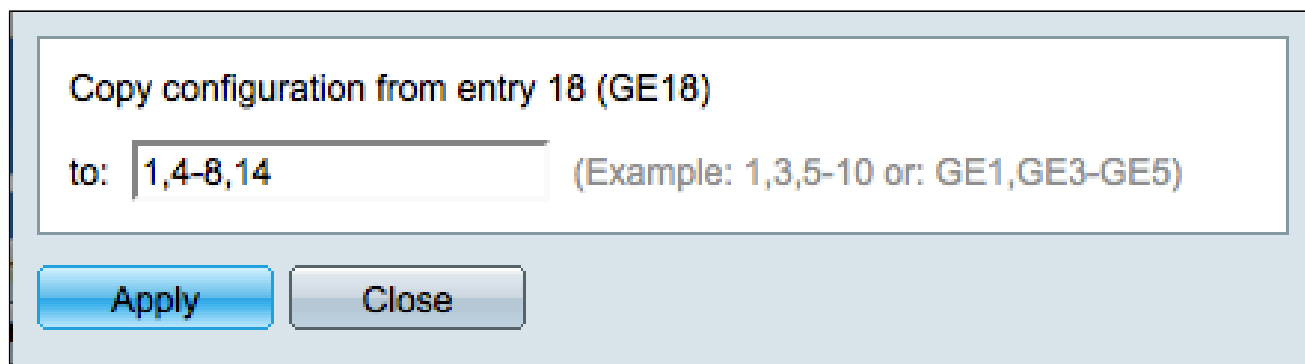
·啟用 — 即使資料包與ACL不匹配，也會轉發這些資料包。

步驟 6. 按一下「Apply」，將所選ACL繫結到介面。Edit ACL Binding視窗關閉。

步驟7. (可選) 選中所需介面的覈取方塊，然後按一下清除，解除該介面與ACL的繫結。



步驟8. (可選) 選中所需介面的覈取方塊，然後按一下Copy Settings將該介面的設定複製到其他介面。此時會顯示「複製設定」視窗：



步驟 9. 輸入要複製所選連線埠設定的連線埠的連線埠號碼或連線埠名稱。

步驟 10. 按一下「Apply」以應用設定，或按一下「Close」以取消設定。

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）。