300系列託管交換器上的網際網路控制訊息通訊協定(ICMP)篩選組態

目標

網際網路控制訊息通訊協定(ICMP)是一種網路層通訊協定，用於報告和通知錯誤以及網路探索。使用ICMP可以在網路上執行許多攻擊。例如，ICMP泛洪拒絕服務(DoS)攻擊是利用ICMP協定漏洞和網路配置不正確的攻擊。ICMP過濾是一種解決方案，可防止這些型別的網路攻擊。您可以配置交換機以過濾要阻止ICMP資料包的IP地址或埠。本文說明如何在300系列託管交換器上設定ICMP過濾。

適用裝置

·SF/SG 300系列託管交換器

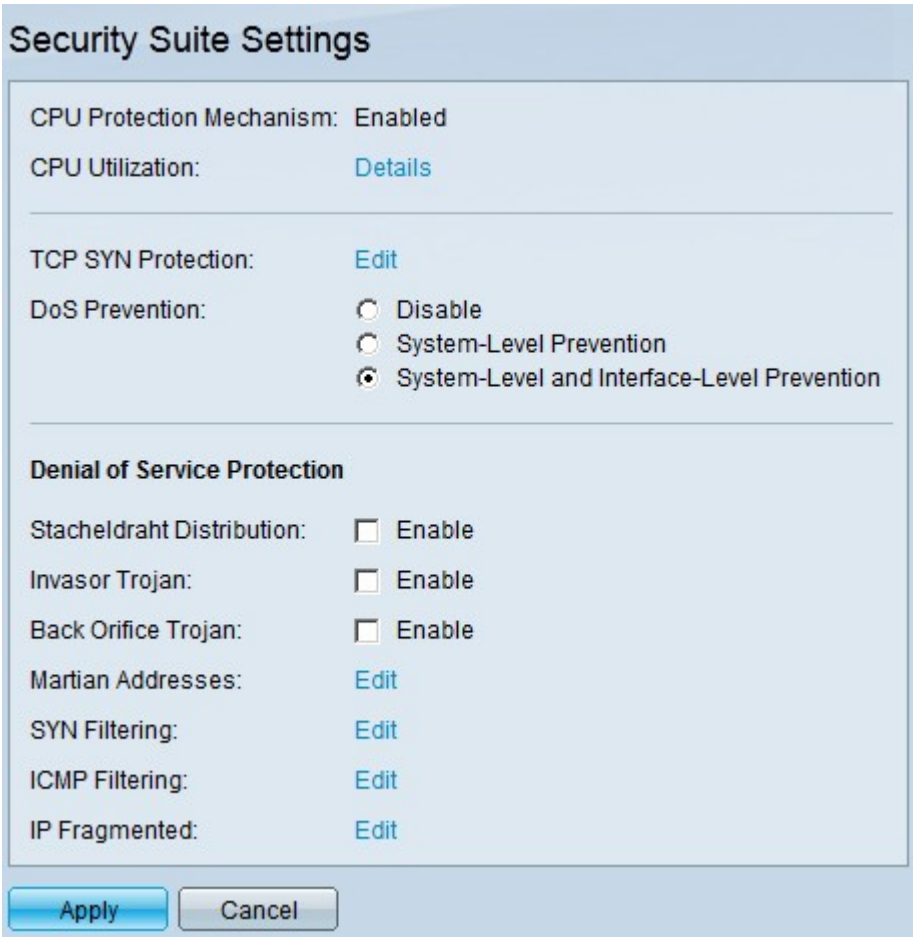
軟體版本

•1.3.0.62

啟用拒絕服務級別預防

要應用ICMP過濾，必須首先確保交換機處於正確的拒絕服務等級保護中。本節介紹如何在300系列託管交換器上啟用正確的防護等級。

步驟1.登入到Web配置實用程式，然後選擇**Security > Denial of Service Prevention > Security Suite Settings**。將開啟*安全套件設定*頁面：



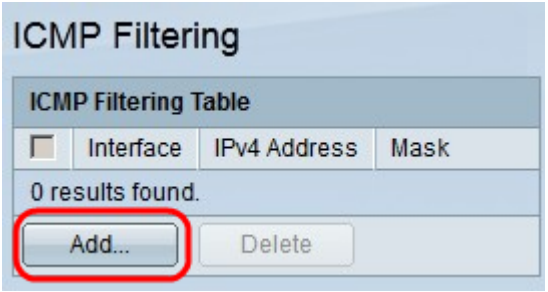
步驟2.在DoS預*防領域*，有三種級別的預防。按一下**System-Level and Interface-Level Prevention**單選按鈕。此級別允許您配置ICMP過濾。

步驟3.按一下**Apply**以儲存組態。

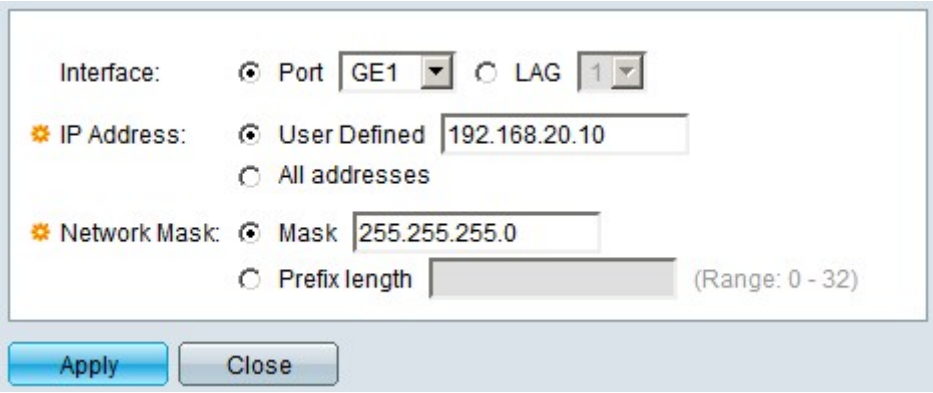
ICMP過濾配置

本節介紹如何在300系列託管交換器上設定ICMP過濾。

步驟1.登入到Web配置實用程式並選擇**Security > Denial of Service Prevention > ICMP Filtering**。*ICMP Filtering*頁面隨即開啟：



步驟2.按一下**Add**。系統將顯示*Add ICMP Filtering*視窗。



步驟3.在*Interface*欄位中，按一下其中一個可用介面選項的單選按鈕：

·連線埠 — 允許您選擇要從中過濾ICMP封包的連線埠。

·LAG — 允許您選擇希望從中過濾ICMP資料包的LAG。LAG將多個埠分組到一個邏輯埠中。

步驟4.在「*IP Address*」欄位中，按一下其中一個可用選項的單選按鈕，以定義要從中過濾ICMP封包的IP位址/位址：

·使用者定義 — 使用者定義的ICMP資料包源。

·所有地址 — 所有IP地址ICMP資料包源範圍。

步驟5在*Network Mask*欄位中，按一下其中一個可用選項的單選按鈕以輸入步驟4中設定的IP位址的網路掩碼：

·掩碼 — 採用點格式的子網掩碼，例如255.255.255.0。

·字首長度 — 斜槓格式的子網掩碼，例如\24。

步驟6.按一下**Apply**以儲存組態。

下圖說明設定之後的變更：

步驟7.（可選）若要刪除ICMP過濾器，請在ICMP過濾表中選中要刪除的ICMP過濾器的覈取方塊，然後點選**刪除**。