300系列託管交換器上的阻斷服務(DoS)IP片段篩選組態

目標

網路流量使用稱為資料包的多個資料包傳送。 每種傳輸方法（乙太網路、權杖環等）都有其可處理的最大資料包大小。 如果資料包對於傳輸方法而言過大，則會將其分割為較小的片段。 此過程稱為IP分段。大多數網路流量不必進行分段。事實上，已分段流量可能會被用作拒絕服務(DoS)攻擊。 DoS攻擊會向網路泛洪虛假流量，並減緩或停止網路。300系列託管交換機可以阻止IP片段，從而降低網路遭受DoS攻擊的脆弱性。本文說明如何在300系列托*管交換器*上設定IP片段篩選設定。

附註：僅當啟用DoS防護時，才能使用IP片段過濾器。 請參閱*300系列託管交換機上的安全套件設定*一文以獲得幫助。

適用裝置

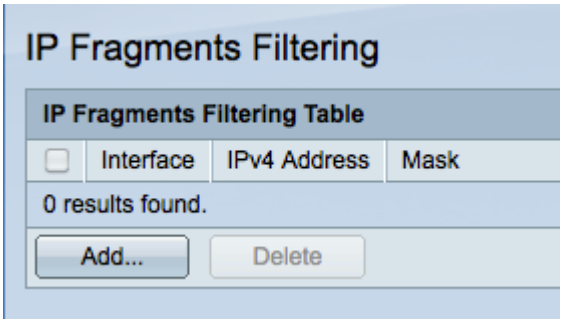
·SF/SG 300系列託管交換器

軟體版本

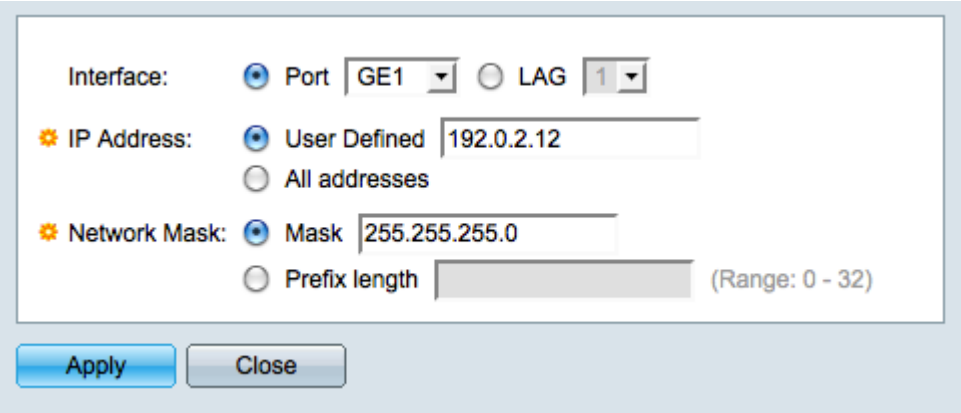
•1.3.0.62

新增IP片段過濾器

步驟1.登入到Web配置實用程式，然後選擇**Security > Denial Of Service Prevention > IP Fragments Filtering**。將開啟*IP Fragments Filtering*頁面：



步驟2.按一下**Add**以新增一個IP片段過濾器。系統將顯示*Add IP Fragments Filtering*視窗。



步驟3.在Interface欄位中點選與所需介面對應的單選按鈕。 這是將分配過濾器的物理位置。

·連線埠 — 交換器上的實體連線埠。 從Port下拉選單中選擇特定埠。

·LAG — 充當單個埠的一組埠。 從LAG下拉選單中選擇特定LAG。

步驟4.點選與IP Address欄位中要過濾的所需IPv4地址對應的單選按鈕。

·使用者定義 — 輸入要過濾的IP地址。

·所有地址 — 過濾所有IPv4地址。

附註：如果您在步驟4中選擇了「所有地址」，請跳到步驟6。

步驟5.點選與Network Mask欄位中用於定義IP地址子網掩碼的方法對應的單選按鈕。

·掩碼 — 在網路掩碼欄位中輸入網路掩碼。

·字首長度(Prefix Length) — 在「字首長度」(Prefix length)欄位中輸入字首長度（介於0到32之間的整數）。

步驟6.按一下**Apply**以儲存變更，然後按一下**Close**以關閉*Add IP Fragments Filtering*視窗。