300系列託管交換器上的阻斷服務(DoS)SYN篩選組態

目標

拒絕服務(DoS)攻擊會向網路泛洪虛假流量。這會將網路伺服器資源從合法使用者那裡抽走。SYN泛洪特別針對TCP協定。TCP協定的運行需要三個步驟。首先，使用者將其IP地址傳送到伺服器並請求連線。接下來，伺服器響應請求並等待確認。最後，使用者確認伺服器已開啟連線。TCP SYN攻擊使用多個IP地址請求連線，但一旦連線開啟，就永遠不會向伺服器傳送確認。伺服器在開始丟棄TCP請求之前，只能開啟有限數量的連線，即使合法使用者也如此。

TCP流量通過多個虛擬埠傳送。這些埠用於將網路流量拆分為通用組。可以將SYN過濾器配置為阻止來自特定虛擬埠的流量。此外，SYN過濾是在交換機的實際物理埠或LAG上配置的。本文介紹如何在300系列託管交換機上配置SYN過濾。

附註：只有啟用DoS防護時，才能使用Syn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

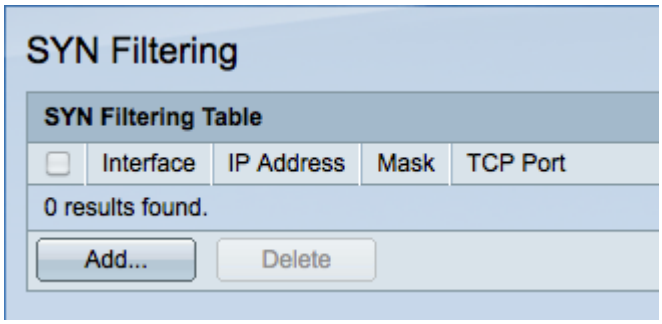
·SF/SG 300系列託管交換器

軟體版本

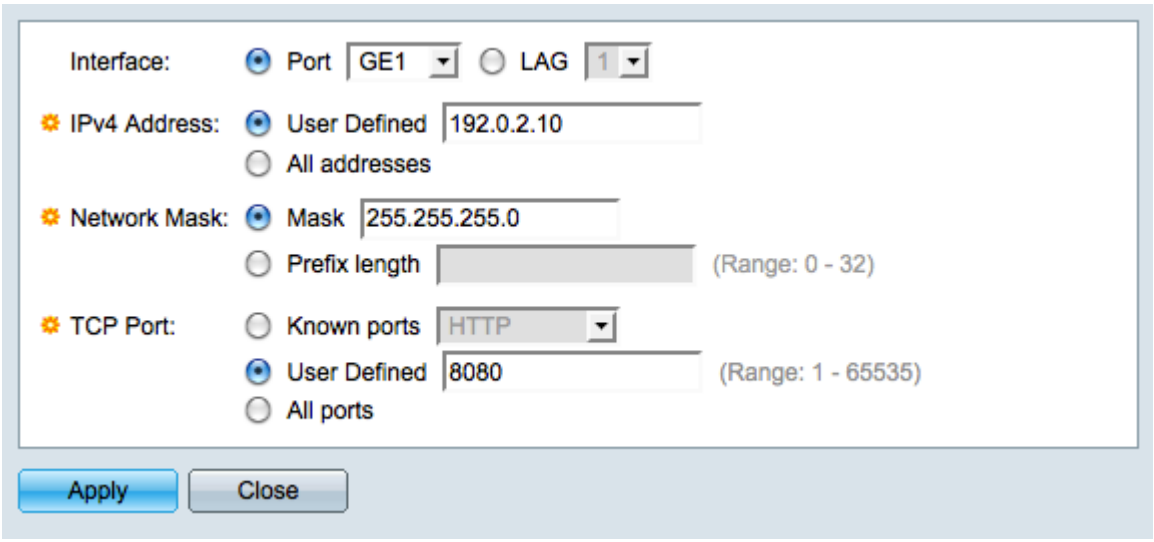
·v1.2.7.76

SYN過濾配置

步驟1.登入到Web配置實用程式，然後選擇**Security > Denial of Service Prevention > SYN Filtering**。*SYN Filtering*頁面開啟：



步驟2.按一下**Add**新增新的SYN過濾器。出現*Add Syn 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「IPv4地址」欄位中所需的IPv4地址對應的單選按鈕。

·使用者定義 — 輸入要過濾的TCP流量的IP地址。

·所有地址 — 針對TCP流量過濾所有IPv4地址。如果已選擇所有地址，請跳至步驟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.在TCP Port欄位中點選與要過濾的所需TCP埠對應的單選按鈕。這些是網路流量所劃分的虛擬埠。

·已知埠 — 從已知埠下拉選單中選擇要過濾的TCP埠。

·使用者定義 — 輸入要過濾的TCP埠。

·所有埠 — 所有TCP埠都經過過濾。

步驟7.按一下**Apply**以儲存變更，然後按一下**Close**以退出**Add Syn Filtering**視窗。