

在300系列託管交換器上同步(SYN)篩選組態

目標

TCP是一種傳輸層協定，它提供可靠、有序的資料包傳輸，還允許檢測錯誤和丟失資料以觸發重新傳輸，直到正確完整地接收資料。在客戶端傳送資料之前，它會向伺服器請求一個帶有同步(SYN)資料包的連線以啟動連線。然後伺服器向客戶端傳送SYN和確認(ACK)資料包，客戶端傳送ACK資料包以確認伺服器響應。在客戶端與伺服器之間的三次握手連線之後，可以傳送資料。

此TCP三次握手中斷時，會發生SYN泛洪攻擊。惡意客戶端使用SYN資料包向伺服器泛洪，伺服器使用SYN和ACK資料包響應所有惡意客戶端請求，但惡意客戶端不會傳送回ACK資料包。伺服器會等待根本無法到達的ACK資料包，這將佔用合法使用者的伺服器資源，並最終導致網路癱瘓。SYN過濾可防止這些攻擊。本文介紹如何在300系列託管交換機上配置SYN過濾。

適用裝置

- SF/SG 300系列託管交換器

軟體版本

- v1.2.7.76

啟用拒絕服務級別預防

要應用SYN過濾，首先需要確保交換機處於正確的拒絕服務等級預防中。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：

Security Suite Settings

CPU Protection Mechanism: Enabled
CPU Utilization: [Details](#)

TCP SYN Protection: [Edit](#)
DoS Prevention: Disable
 System-Level Prevention
 System-Level and Interface-Level Prevention

Denial of Service Protection

Stacheldraht Distribution: Enable
Invasor Trojan: Enable
Back Orifice Trojan: Enable
Martian Addresses: [Edit](#)
SYN Filtering: [Edit](#)
ICMP Filtering: [Edit](#)
IP Fragmented: [Edit](#)

[Apply](#) [Cancel](#)

步驟2. 在DoS預防領域，有三種預防級別。按一下「**System-Level and Interface-Level Prevention**」。此級別允許您配置SYN過濾。

步驟3. 按一下**Apply**以儲存組態。

篩選TCP SYN封包

本節介紹如何在300系列託管交換器上設定SYN篩選。

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：

SYN Filtering

SYN Filtering Table				
<input type="checkbox"/>	Interface	IP Address	Mask	TCP Port
0 results found.				
Add...		Delete		

步驟2. 按一下**Add**。出現*Add SYN 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 — 允許您從連線埠下拉式清單中選擇要從中篩選SYN封包的連線埠。
- LAG — 允許您從鏈路聚合組(LAG)下拉選單中選擇要從中過濾SYN資料包的LAG。LAG將多個埠分組到一個邏輯埠中。

步驟4.在IPv4 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SYN資料包的IPv4地址/地址：

- 使用者定義 — 允許輸入定義SYN封包過濾器的IPv4位址。
- 所有地址 — 此選項過濾SYN資料包的所有IPv4地址。

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中配置的IP位址的網路掩碼：

- 掩碼 — 此選項可讓您輸入IP地址的子網掩碼。
- 字首長度 — 此選項可讓您以字首格式輸入子網掩碼IP地址。

步驟5.在「TCP Port」欄位中，按一下其中一個可用選項，以確定要篩選的TCP連線埠：

- 已知埠 — 此選項可讓您從「已知埠」下拉選單中選擇埠。例如，HTTP是80,TELNET是23。
- 使用者定義 — 此選項可讓您輸入要過濾的TCP埠號。
- 所有埠 — 此選項過濾所有TCP埠。

步驟6.按一下**Apply** 以儲存組態。對SYN過濾表進行更改：

SYN Filtering				
SYN Filtering Table				
<input type="checkbox"/>	Interface	IP Address	Mask	TCP Port
<input type="checkbox"/>	GE1	192.168.20.10	255.255.255.0	All
<input type="button" value="Add..."/>		<input type="button" value="Delete"/>		

步驟7. (可選) 要刪除SYN過濾器，請在SYN過濾表中選中您要刪除的SYN過濾器的覈取方塊

。然後按一下「Delete」。