# 300系列託管交換器上的安全套件設定

## 目標

Cisco 300系列託管交換機上的安全套件提供針對拒絕服務(DoS)攻擊的保護。DoS攻擊以虛假流量泛洪網路，導致網路伺服器資源不可用或對合法使用者無響應。一般來說，DoS攻擊有兩種型別。暴力DoS攻擊會泛洪伺服器，消耗伺服器和網路頻寬。系統攻擊利用協定漏洞（如TCP SYN消息）使系統崩潰。本文說明300系列託管交換器上的安全套件中可用的設定。

**附註：**啟用DoS攻擊保護後，訪問控制清單(ACL)和高級QoS策略在埠上處於非活動狀態。

## 適用裝置

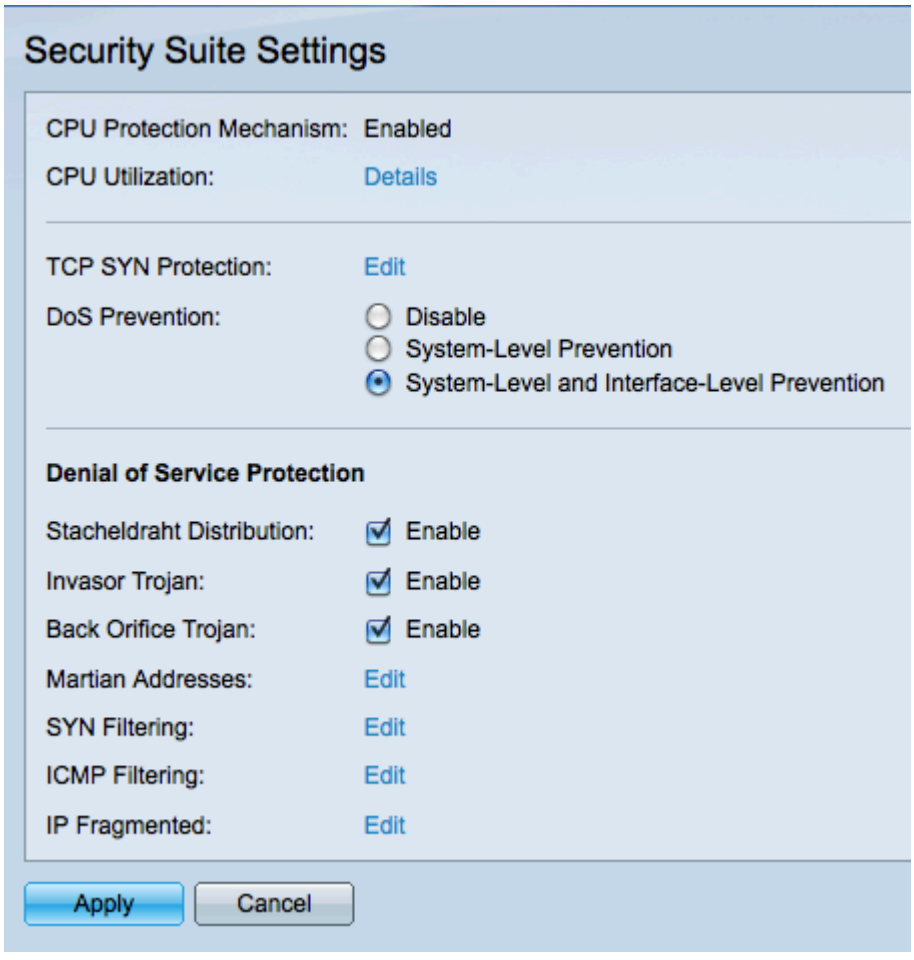
·SF/SG 300系列託管交換器

## 軟體版本

•1.3.0.62

## 安全套件設定配置

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：




**附註：**300系列託管交換機上預設啟用CPU保護機制，因此無法禁用。交換器使用安全核心技

術(SCT)，無論收到多少總流量，它都允許交換器處理管理和通訊協定流量。

步驟2.（可選）在「CPU Utilization」欄位中按一下**Details**以檢視CPU利用率。如需詳細資訊，請參閱*200/300系列託管交換器上的CPU使用率*一文。

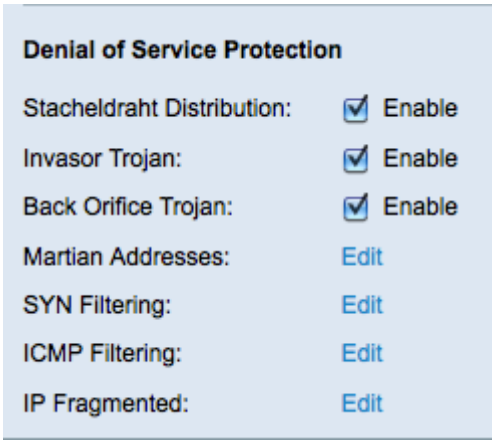
步驟3.（可選）在TCP SYN Protection欄位中按一下**Edit**，編輯TCP SYN Protection設定。如需詳細資訊，請參閱*300系列託管交換器上的同步(SYN)篩選組態*一文。

步驟4.在DoS Prevention欄位中，點選與您要使用的DoS預防方法對應的單選按鈕。可用選項包括：

·禁用 — 禁用DoS保護功能。如果選擇Disable，請跳至步驟13。

·系統 — 級別保護 — 啟用DoS保護功能，可保護Invasor特洛伊木馬程式、Stacheldraht Distribution、Back Orifice特洛伊木馬程式和火星地址不受影響。

·系統 — 級別預防和介面級別保護 — 啟用在拒絕服務保護區域中定義的所有安全措施。




步驟5.選中Stacheldraht Distribution欄位中的**Enable**覈取方塊以丟棄源TCP埠號為16660的TCP資料包。

步驟6.選中Invasor特洛伊木馬欄位中的**Enable**覈取方塊，以丟棄目標TCP埠為2140且源TCP埠為1024的TCP資料包。

步驟7.選中Back Orifice特洛伊木馬欄位中的**Enable**覈取方塊，以丟棄目標UDP埠等於31337且源UDP埠為1024的UDP資料包。

**附註：**雖然有數百個DoS攻擊，但上述埠通常被惡意活動利用。但是，它們也用於合法流量。如果您的裝置使用上述任何埠，則該資訊將被阻止。

步驟8.在Martian Addresses欄位中點選**Edit**以編輯Martian Addresses表。火星地址表丟棄來自選定IP地址的資料包。要編輯火星地址清單，請參閱*300系列託管交換機上的拒絕服務(DoS)火星地址配置*一文。

**附註：**步驟9-12要求在步驟4中選擇系統級別和介面級別預防。如果您選擇了其他DoS預防型別，請跳至步驟13。

步驟9.在SYN Filtering欄位中點選**Edit**，允許管理員阻止某些TCP埠。要配置SYN過濾，請參閱*300系列託管交換機上的拒絕服務(DoS)SYN過濾配置*一文。

步驟10.在SYN Rate Protection欄位中按一下**Edit**，以限制接收的SYN資料包數。要配置SYN速率保護，請參閱*300系列託管交換機上的SYN速率保護*一文。

步驟11.在ICMP Filtering欄位中點選**Edit**，以允許阻止來自某些來源的ICMP資料包。要配置ICMP過濾，請參閱*300系列託管交換機上的網際網路控制消息協定(ICMP)過濾配置。*

步驟12.在「IP分段的」欄位中按一下**Edit**，以封鎖分段的IP封包。要配置IP片段過濾，請參閱*300系列託管交換器上的拒絕服務(DoS)IP片段過濾配置*一文。

步驟13.按一下**Apply**儲存更改，或按一下**Cancel**取消更改。