在Sx500系列堆疊式交換器上設定拒絕服務防禦技術（安全套件）

目標

拒絕服務(DoS)或分散式拒絕服務(DDoS)攻擊會限制有效使用者使用網路。攻擊者通過向網路泛洪大量佔用網路所有頻寬的不必要請求來執行DOS攻擊。DoS攻擊可以減緩網路速度，或者使網路完全中斷幾個小時。DoS保護是提高網路安全性的主要特徵；偵測異常流量並進行過濾。

本文說明在安全套件設定上配置拒絕服務以及用於防止拒絕服務的多種技術。

注意：如果選擇的DoS防護是系統級和介面級防護，則可以編輯和配置軍事地址、SYN過濾、SYN速率保護、ICMP過濾和IP片段過濾。本文還將對這些配置進行說明。

附註：在啟用DoS防護之前，必須取消繫結所有訪問控制清單(ACL)或配置到埠的任何高級QoS策略。在埠上啟用DoS保護後，ACL和高級QoS策略將處於非活動狀態。

適用裝置

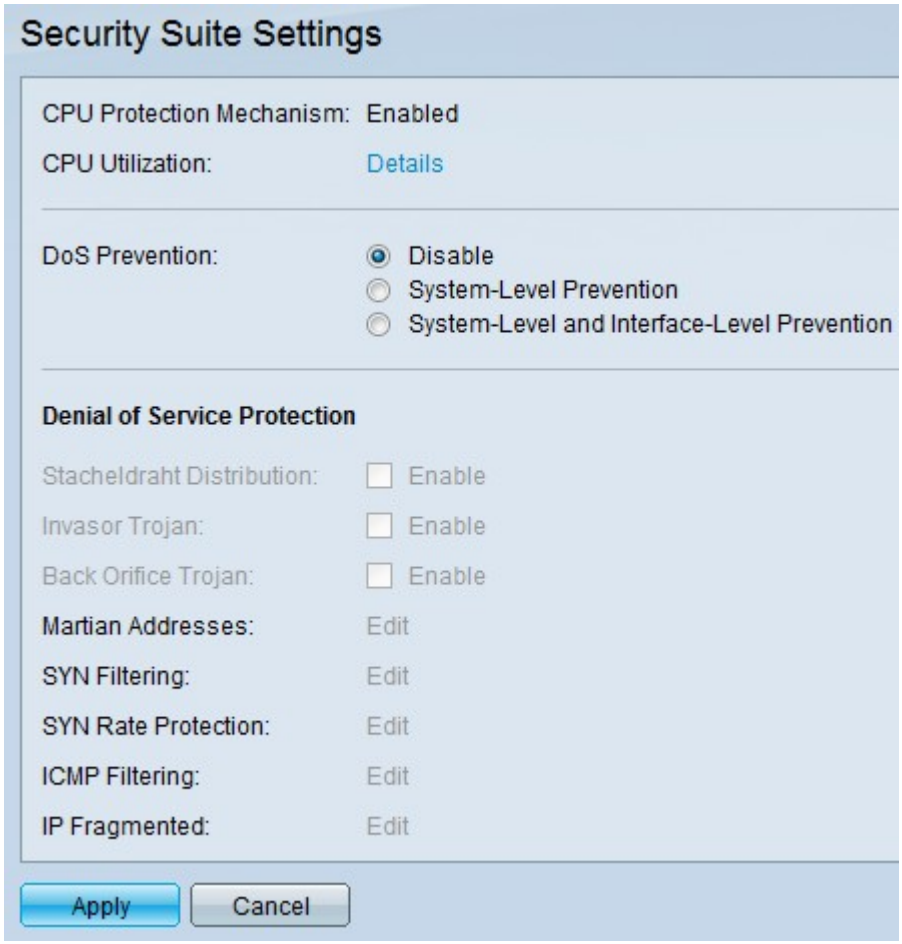
- Sx500系列堆疊式交換器

軟體版本

- 1.3.0.62

在安全套件設定上配置拒絕服務

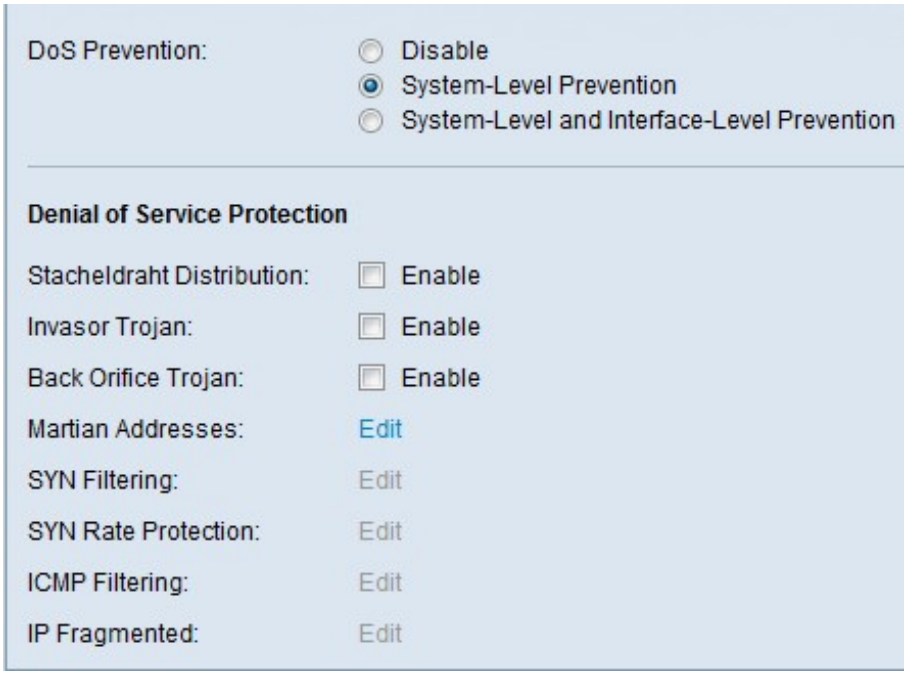
步驟1.登入到Web配置實用程式，然後選擇**Security > Denial of Service Prevention > Security Suite Settings**。將開啟*安全套件設定*頁面：



- CPU保護機制 — 這是
- **已啟用**.這表示已啟用安全轉換工具(SCT)。
- CPU利用率 — 按一下
- **檢視**CPU資源利用率資訊的CPU利用率旁的詳細資訊。

步驟2.按一下DoS Prevention欄位下的相應單選按鈕。

- Disable — 停用DoS預防。
- 系統級防禦 — 可防止Stacheldraht Distribution、Invasor特洛伊木馬和Back Orifice特洛伊木馬的攻擊。
- 系統級和介面級防禦 — 可防止交換器上每個介面的攻擊。



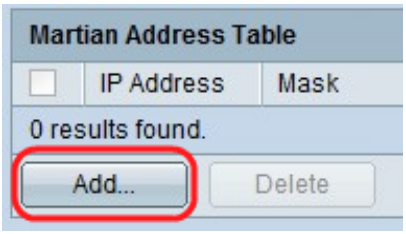
步驟3.可以選擇以下選項進行拒絕服務保護：

- Stacheldraht Distribution — 這是DDoS攻擊的示例，攻擊者使用客戶端程式連線到網路內部的電腦。然後，這些電腦向內部伺服器發出多個登入請求並啟動DDoS攻擊。
- 入侵者特洛伊木馬 — 如果電腦受到此攻擊的感染，則TCP埠2140用於惡意活動。
- Back Orifice特洛伊木馬 — 丟棄用於與伺服器和客戶端程式通訊以進行DoS攻擊的UDP資料包。

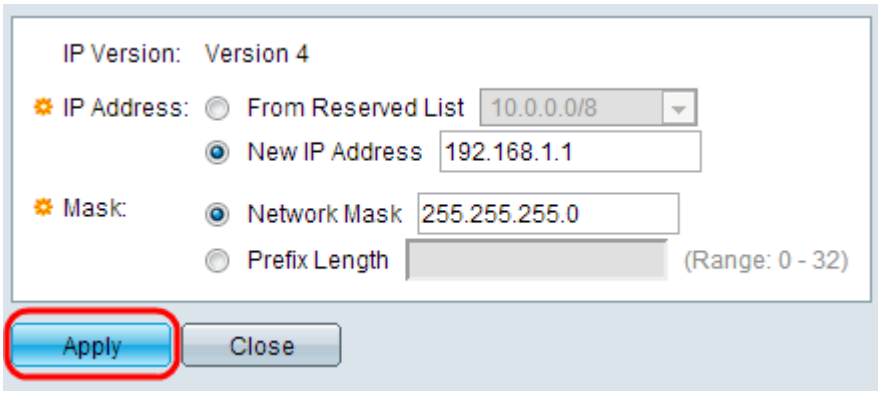
火星地址配置

步驟1.在「火星地址」(Martian Addresses)欄位中按一下**編輯**，然後開啟「火星地址」(*Martian Addresses*)頁面。火星地址表示可能導致網路攻擊的IP地址。來自這些網路的封包會遭捨棄。

步驟2.選中**Include**到Reserved Martian Addresses中，然後按一下**Apply**，在System Level Prevention清單中新增Reserved Martian Addresses。



步驟3.要新增火星地址，請按一下**Add**。將顯示*Add Martian Addresses*頁。輸入以下引數：



步驟4.在「IP地址」欄位中輸入需要拒絕的IP地址。

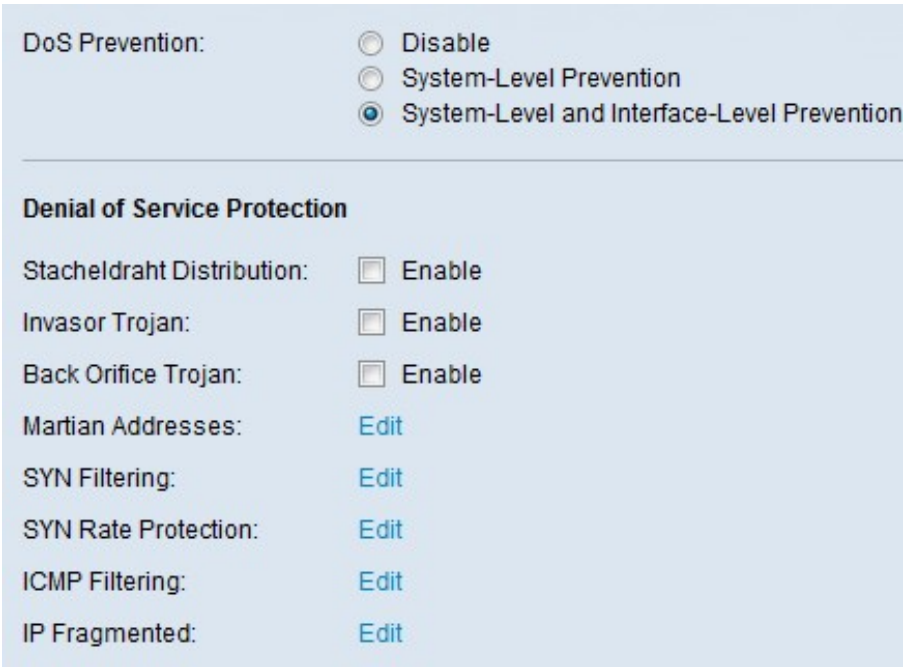
步驟5. IP地址掩碼，表示應拒絕的IP地址範圍。

- IP版本 — 支援的IP版本。目前僅允許IPv4。
- 從保留清單 — 從保留清單中選擇已知的IP地址。
- 新IP地址 — 輸入IP地址。
- 網路掩碼 — 點分十進位制格式的網路掩碼。
- 字首長度 — IP地址的字首，用於定義啟用拒絕服務防禦的IP地址範圍。

步驟6.按一下**Apply**，將火星地址寫入到執行組態檔中。

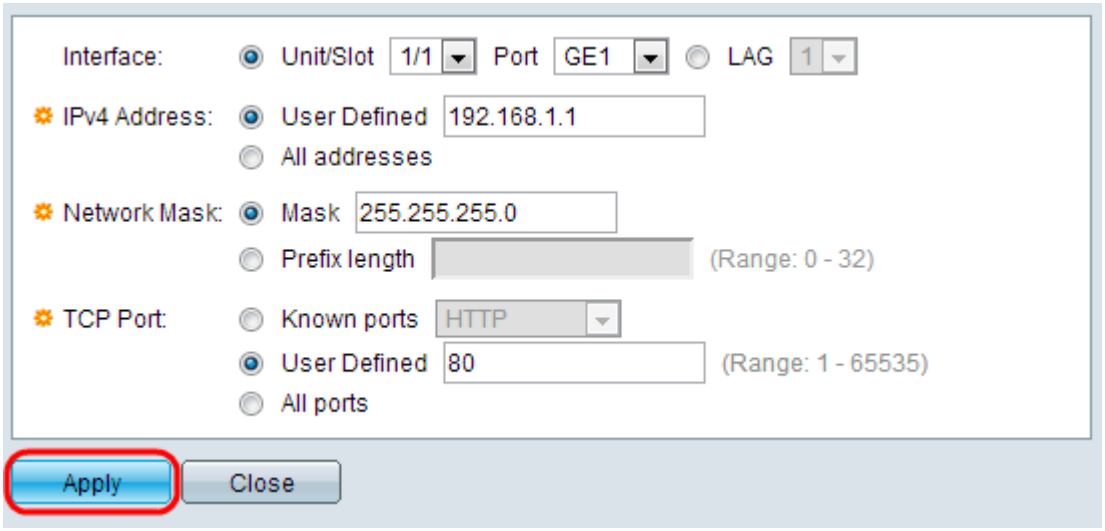
SYN過濾的配置

SYN過濾允許網路管理員丟棄帶有SYN標誌的非法TCP資料包。SYN埠過濾是基於每個埠定義的。



步驟1。若要設定SYN篩選，請按一下「**Edit**」，*SYN Filtering*頁面隨即開啟：

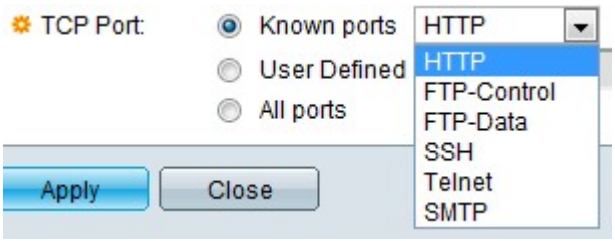
步驟2.按一下**Add**。螢幕上會顯示*Add SYN filtering*頁面。在顯示的欄位中輸入以下引數：



步驟3.選擇需要在其上定義過濾器的介面。

步驟4.按一下**User Defined**以提供一個定義了過濾器的IP地址，或按一下**All Addresses**。

步驟5.啟用過濾器的網路遮罩。按一下「**Prefix Length**」以指定長度，其範圍為0到32，或按一下「**Mask**」以輸入以點分十進位記法表示的子網掩碼。



步驟6.按一下要過濾的目標TCP埠。它們屬於以下型別：

- 已知連線埠 — 從清單中選擇連線埠。
- 使用者定義 — 輸入埠號。
- 所有埠 — 按一下以指示已過濾所有埠。

步驟7.按一下**Apply**，即可將SYN篩選寫入執行組態檔。

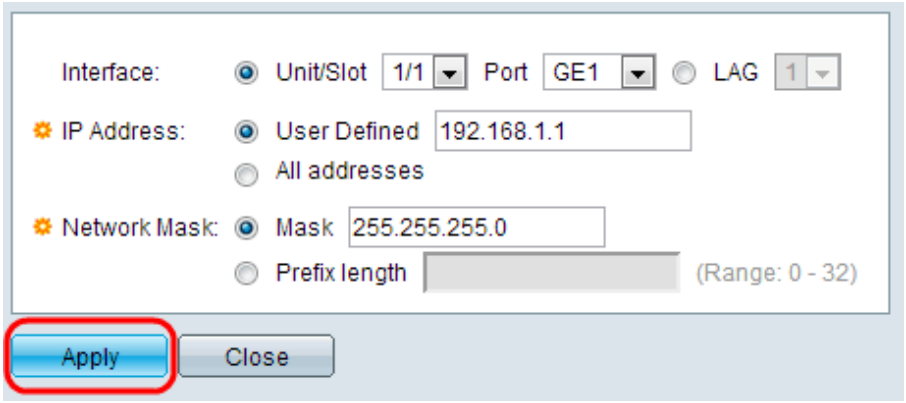
ICMP過濾的配置

網際網路控制訊息通訊協定(ICMP)是最重要的網際網路通訊協定之一。它是網路層協定。作業系統使用ICMP傳送錯誤消息，告知所請求的服務不可用或無法訪問特定主機。它還用於傳送診斷消息。不能使用ICMP在系統之間交換資料。它們通常是針對IP資料包中的某些錯誤而產生的。

ICMP流量是非常重要的網路流量，但如果惡意攻擊者將其用於網路，它也會導致許多網路問題。這就需要嚴格過濾來自Internet的ICMP流量。*ICMP過濾*頁面啟用過濾來自特定來源的ICMP資料包。這樣可以在發生任何ICMP攻擊的情況下將網路上的負載降至最低。

步驟1。若要設定ICMP過濾，請按一下**Edit**，然後*ICMP過濾*頁面隨即開啟。

步驟2.按一下**Add**。此時會顯示*Add ICMP Filtering*頁面。在顯示的欄位中輸入以下引數：



步驟3.選擇定義ICMP過濾的介面。

步驟4.輸入已啟用ICMP封包過濾的IPv4位址，或按一下**All Addresses**以封鎖來自所有來源位址的ICMP封包。如果輸入了IP地址，請輸入掩碼或字首長度。

步驟5.啟用速率保護的網路掩碼。選擇源IP地址的網路掩碼的格式，然後按一下其中一個欄位。

- 掩碼 — 選擇源IP地址所屬的子網，並以點分十進位制格式輸入子網掩碼。
- 按一下**Prefix Length**以指定長度並輸入由來源IP位址首碼組成的位元數，其範圍從0到32。

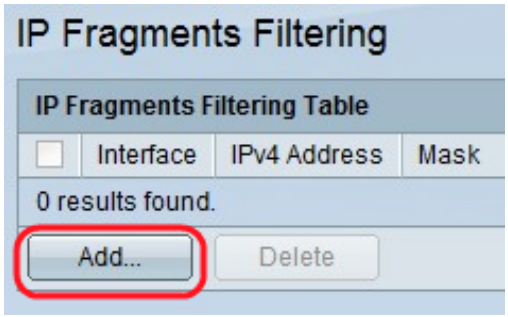
步驟6.按一下**Apply**，即可將ICMP篩選寫入執行組態檔。

IP片段篩選的組態

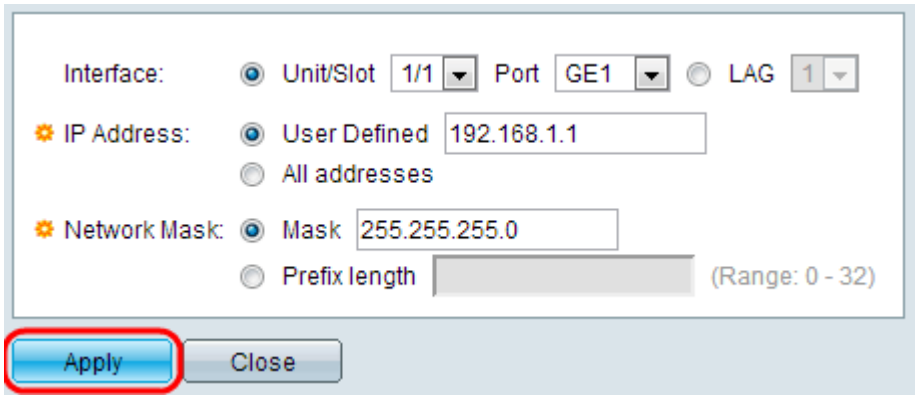
所有封包都有一個最大傳輸單位(MTU)大小。MTU是網路可以傳輸的最大封包的大小。IP利用分段的優點，因此可形成透過連結、MTU小於原始封包大小的封包。因此，大小大於鏈路可允許的MTU的資料包必須分成較小的資料包，以允許它們通過鏈路。

另一方面，碎片化也會帶來許多安全問題。因此，必須阻止IP片段，因為有時它們可能是系統受損的原因。

步驟1。若要設定IP片段篩選，請按一下**Edit**，然後*ICMP Fragments Filtering*頁面隨即開啟。



步驟2.按一下**Add**。螢幕上會顯示*Add IP Fragment Filtering*頁面。在顯示的欄位中輸入以下引數：



步驟3.介面 — 選擇定義IP分段的介面。

步驟4. IP地址 — 輸入已啟用IP分段的IP地址，或按一下**All Addresses**以阻止來自所有源地址的IP分段資料包。如果輸入了IP地址，請輸入掩碼或字首長度。

步驟5.網路遮罩 — IP分段遭封鎖的網路遮罩。選擇源IP地址的網路掩碼的格式，然後按一下其中一個欄位。

- 掩碼 — 選擇源IP地址所屬的子網，並以點分十進位制格式輸入子網掩碼。
- 按一下**Prefix Length**以指定長度並輸入由來源IP位址首碼組成的位元數，其範圍從0到32。

步驟6.按一下Apply以將IP片段篩選功能寫入執行組態檔。