Configurazione delle tecniche di prevenzione della negazione del servizio (Security Suite) sugli switch impilabili serie Sx500

Obiettivo

Gli attacchi DoS (Denial of Service) o DDoS (Distributed Denial of Service) limitano gli utenti validi per l'utilizzo della rete. L'aggressore esegue un attacco DOS inondando una rete con molte richieste non necessarie che occupano tutta la larghezza di banda della rete. Gli attacchi DoS possono rallentare una rete o arrestare completamente una rete per diverse ore. La protezione DoS è la caratteristica principale per migliorare la sicurezza della rete. rileva il traffico anomalo e lo filtra.

In questo articolo viene illustrata la configurazione di Denial of Service nelle impostazioni della suite di sicurezza e vengono illustrate diverse tecniche utilizzate per la prevenzione.

Nota: se la prevenzione DoS scelta è a livello di sistema e a livello di interfaccia, è possibile modificare e configurare gli indirizzi marziali, il filtro SYN, la protezione della velocità SYN, il filtro ICMP e il filtro IP Fragment. In questo articolo vengono spiegate anche queste configurazioni.

Nota: Prima di attivare la prevenzione DoS, è necessario dissociare tutti gli Access Control Lists (ACL) o qualsiasi criterio QoS avanzato configurato per la porta. I criteri ACL e QoS avanzati non sono attivi quando la protezione DoS è abilitata sulla porta.

Dispositivi interessati

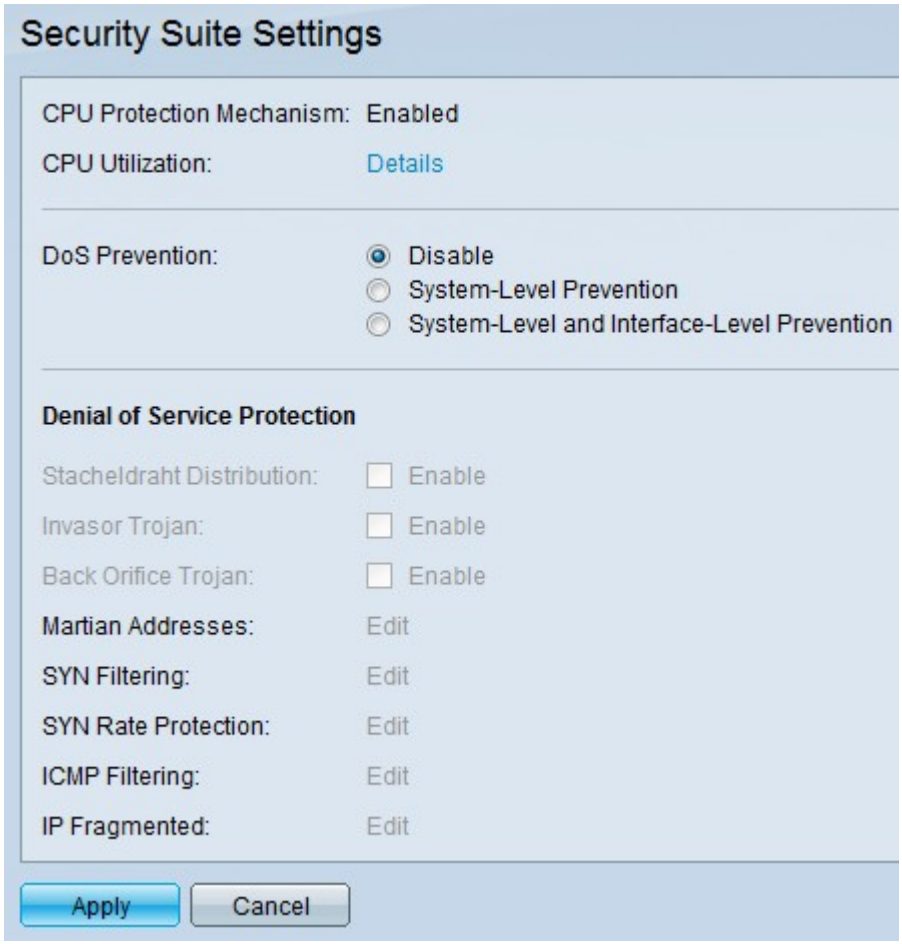
- Serie Sx500 Stackable Switch

Versione del software

- 1.3.0.62

Configurazione di Denial of Service nelle impostazioni della suite di sicurezza

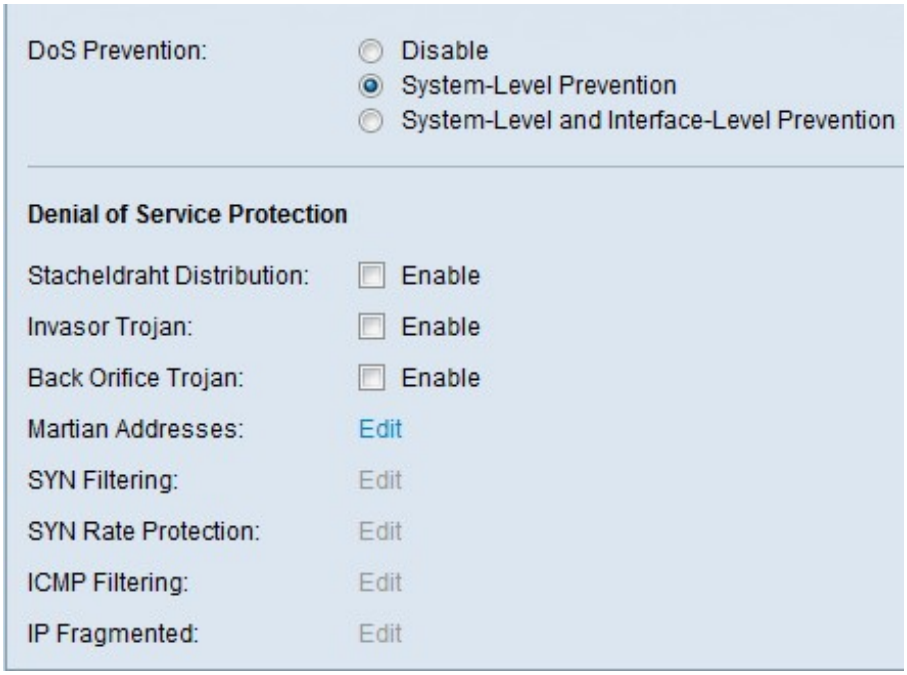
Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Prevenzione della negazione del servizio > Impostazioni della suite di sicurezza**. Viene visualizzata la pagina *Impostazioni suite di sicurezza*:



- Meccanismo di protezione della CPU:
- **Attivato**. Ciò indica che lo Security Conversion Tool (SCT) è abilitato.
- Utilizzo CPU - Fare clic su
- **Dettagli** accanto all'utilizzo CPU per visualizzare le informazioni sull'utilizzo delle risorse CPU.

Passaggio 2. Fare clic sul pulsante di opzione appropriato nel campo Prevenzione DoS.

- Disabilita - Consente di disabilitare la prevenzione DoS.
- Prevenzione a livello di sistema: previene gli attacchi da Distribuzione Stacheldraht, Trojan Invasor e Trojan Back Orifice.
- Prevenzione a livello di sistema e di interfaccia: previene gli attacchi per interfaccia sullo switch.



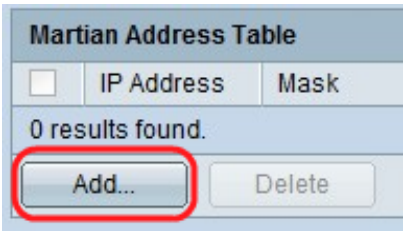
Passaggio 3. Per la protezione da attacchi Denial of Service è possibile scegliere le opzioni seguenti:

- Distribuzione Stacheldraht: questo è un esempio di attacco DDoS in cui l'autore dell'attacco utilizza un programma client per connettersi ai computer della rete. Tali computer inviano quindi più richieste di accesso al server interno e avviano un attacco DDoS.
- Invasor Trojan: se il computer è infetto da questo attacco, la porta TCP 2140 viene utilizzata per attività dannose.
- Back Orifice Trojan — scarta i pacchetti UDP utilizzati per comunicare con il server e il programma client per attacchi DoS.

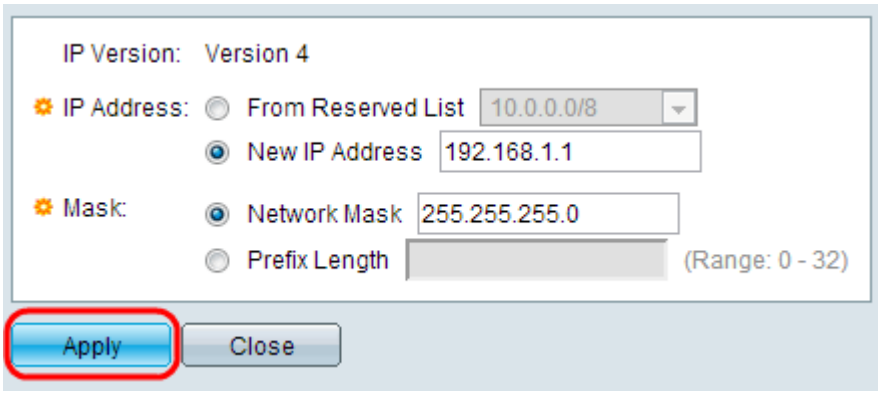
Configurazione degli indirizzi di Martian

Passaggio 1. Fare clic su **Modifica** nel campo Indirizzi marziani, quindi viene visualizzata la pagina *Indirizzi marziani*. Gli indirizzi di Martian indicano l'indirizzo IP che potrebbe essere la causa di un attacco alla rete. I pacchetti provenienti da queste reti vengono scartati.

Passaggio 2. Selezionare **Includi** negli indirizzi riservati di Marziano e fare clic su **Applica** per aggiungere gli indirizzi riservati di Marziano nell'elenco Prevenzione a livello di sistema.



Passaggio 3. Per aggiungere un indirizzo Marziano, fare clic su **Add**. Viene visualizzata la pagina *Aggiungi indirizzi* marziani. Immettere i seguenti parametri:



Passaggio 4. Nel campo Indirizzo IP immettere l'indirizzo IP che deve essere rifiutato.

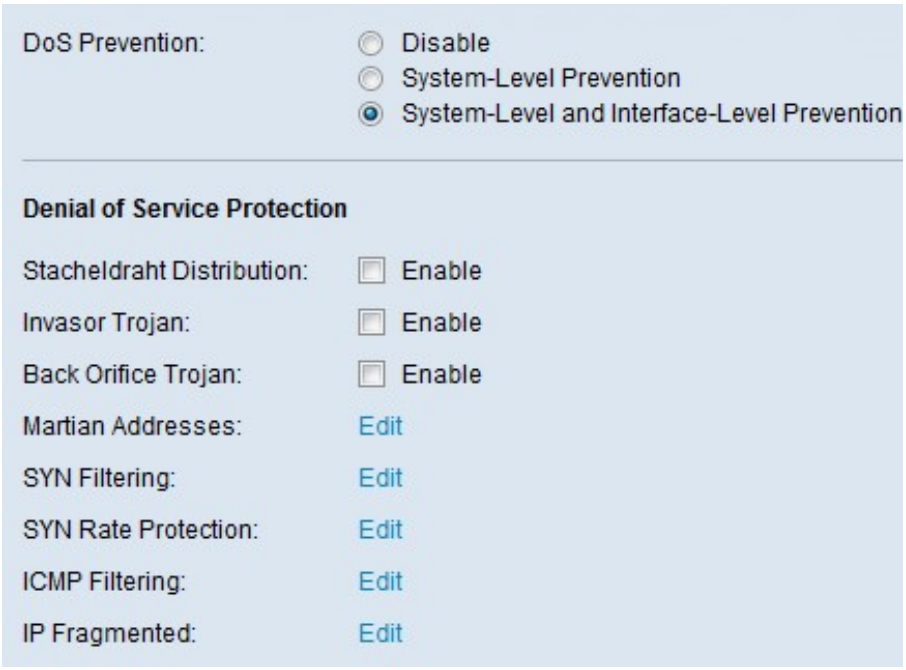
Passaggio 5. Maschera dell'indirizzo IP per indicare l'intervallo di indirizzi IP da rifiutare.

- Versione IP — la versione IP supportata. Al momento, è consentito solo l'IPv4.
- Da elenco riservato: scegliere un indirizzo IP noto dall'elenco riservato.
- Nuovo indirizzo IP - Immettere un indirizzo IP.
- Network Mask - Network Mask in formato decimale con punti.
- Lunghezza prefisso — il prefisso dell'indirizzo IP consente di definire l'intervallo di indirizzi IP per cui è abilitata la funzione di prevenzione degli attacchi Denial of Service.

Passaggio 6. Fare clic su **Apply** per scrivere l'indirizzo di Martian nel file della configurazione corrente.

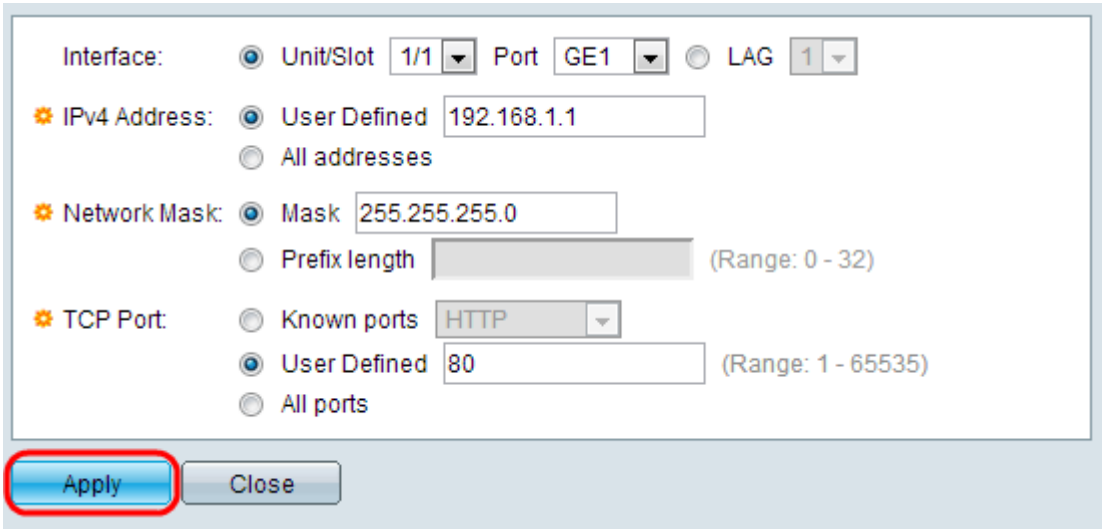
Configurazione del filtro SYN

Il filtro SYN consente agli amministratori di rete di eliminare i pacchetti TCP non validi con il flag SYN. Il filtro della porta SYN è definito per singola porta.



Passaggio 1. Per configurare il filtro SYN, fare clic su **Modifica** per aprire la pagina *Filtro SYN*:

Passaggio 2. Fare clic su **Add**. Viene visualizzata la pagina *Aggiungi filtro SYN*. Immettere i seguenti parametri nei campi visualizzati:

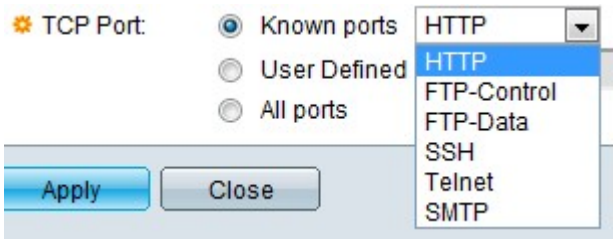


Passaggio 3. Scegliere l'interfaccia su cui definire il filtro.

Passaggio 4. Fare clic su **Definito dall'utente** per specificare un indirizzo IP per il quale è stato definito il filtro oppure fare clic su **Tutti gli indirizzi**.

Passaggio 5. La maschera di rete per cui è abilitato il filtro. Fare clic su **Lunghezza prefisso** per specificare la lunghezza, il suo intervallo è compreso tra 0 e 32, oppure fare clic su

Maschera per immettere la subnet mask come nella notazione decimale puntata.



Passaggio 6. Fare clic sulla porta TCP di destinazione da filtrare. I tipi sono:

- Porte conosciute: scegliere una porta dall'elenco.
- Definito dall'utente: immettere il numero di porta.
- Tutte le porte: fare clic per indicare che tutte le porte sono filtrate.

Passaggio 7. Fare clic su **Apply** (Applica) per scrivere il filtro SYN nel file di configurazione in esecuzione.

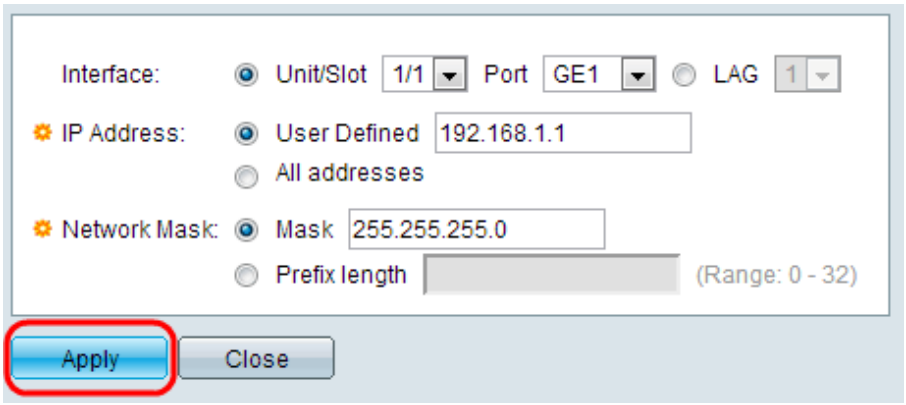
Configurazione del filtro ICMP

Il protocollo ICMP (Internet Control Message Protocol) è uno dei più importanti protocolli Internet. È un protocollo a livello di rete. Il protocollo ICMP viene utilizzato dai sistemi operativi per inviare messaggi di errore per segnalare che il servizio richiesto non è disponibile o che un determinato host non è raggiungibile. Viene anche utilizzato per inviare messaggi diagnostici. Impossibile utilizzare ICMP per lo scambio di dati tra i sistemi. Vengono in genere generati in risposta ad alcuni errori nei datagrammi IP.

Il traffico ICMP è un traffico di rete molto critico ma può anche causare molti problemi di rete se viene utilizzato contro la rete da un utente malintenzionato. Ciò rende necessario filtrare rigorosamente il traffico ICMP proveniente da Internet. La pagina *ICMP Filtering* (Filtro ICMP) abilita il filtro dei pacchetti ICMP da determinate origini. In questo modo si riduce al minimo il carico sulla rete in caso di attacco ICMP.

Passaggio 1. Per configurare il filtro ICMP, fare clic su **Modifica**. Viene visualizzata la pagina *Filtro ICMP*.

Passaggio 2. Fare clic su **Add**. Viene visualizzata la pagina *Aggiungi filtro ICMP*. Immettere i seguenti parametri nei campi visualizzati:



Passaggio 3. Scegliere l'interfaccia su cui è definito il filtro ICMP.

Passaggio 4. Immettere l'indirizzo IPv4 per cui è abilitato il filtro pacchetti ICMP o fare clic su **Tutti gli indirizzi** per bloccare i pacchetti ICMP da tutti gli indirizzi di origine. Se si immette l'indirizzo IP, immettere la lunghezza della maschera o del prefisso.

Passaggio 5. La maschera di rete per cui è abilitata la protezione della velocità. Scegliere il formato della maschera di rete per l'indirizzo IP di origine e fare clic su uno dei campi.

- Maschera — scegliere la subnet a cui appartiene l'indirizzo IP di origine e immettere la subnet mask in formato decimale con punti.
- Fare clic su **Prefix Length** (Lunghezza prefisso) per specificare la lunghezza e immettere il numero di bit che costituiscono il prefisso dell'indirizzo IP di origine. L'intervallo valido è compreso tra 0 e 32.

Passaggio 6. Fare clic su **Apply** (Applica) per scrivere il filtro ICMP nel file di configurazione in esecuzione.

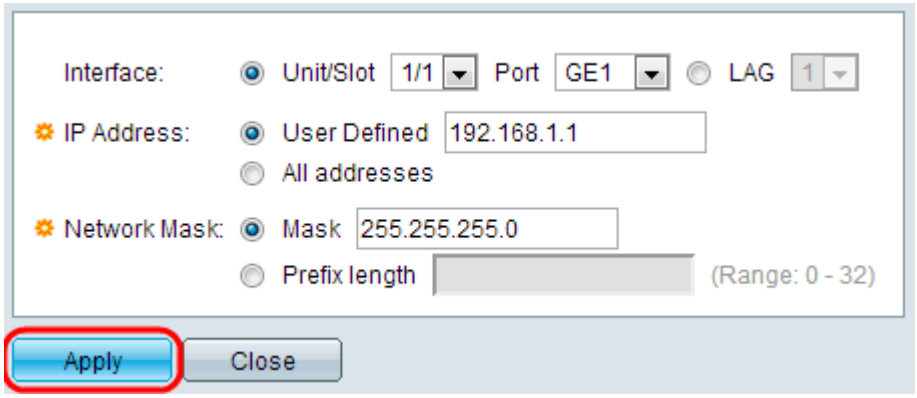
Configurazione del filtro dei frammenti IP

Tutti i pacchetti hanno una dimensione MTU (Maximum Transmission Unit). L'MTU è la dimensione del pacchetto più grande che una rete può trasmettere. Il protocollo IP sfrutta i vantaggi della frammentazione per formare pacchetti che possono attraversare un collegamento con MTU inferiore alle dimensioni originali. Pertanto, i pacchetti le cui dimensioni sono più grandi della MTU consentita del collegamento devono essere divisi in pacchetti più piccoli per consentire loro di attraversare il collegamento.

D'altra parte, la frammentazione può anche porre molti problemi di sicurezza. È quindi necessario bloccare i frammenti IP, poiché a volte possono rappresentare una causa di compromesso nel sistema.

Passaggio 1. Per configurare il filtro dei frammenti IP, fare clic su **Edit** (Modifica). Viene visualizzata la pagina *ICMP Fragments Filtering* (Filtro frammenti ICMP).

Passaggio 2. Fare clic su **Add**. Viene visualizzata la pagina *Add IP Fragment Filtering* (Aggiungi filtro frammenti IP). Immettere i seguenti parametri nei campi visualizzati:



Passaggio 3. Interfaccia: scegliere l'interfaccia su cui definire la frammentazione IP.

Passaggio 4. Indirizzo IP: immettere l'indirizzo IP per il quale è abilitata la frammentazione IP oppure fare clic su **Tutti gli indirizzi** per bloccare i pacchetti IP frammentati da tutti gli indirizzi di origine. Se si immette l'indirizzo IP, immettere la lunghezza della maschera o del prefisso.

Passaggio 5. Network Mask: la maschera di rete per cui è bloccata la frammentazione IP. Scegliere il formato della maschera di rete per l'indirizzo IP di origine e fare clic su uno dei campi.

- Maschera — scegliere la subnet a cui appartiene l'indirizzo IP di origine e immettere la subnet mask in formato decimale con punti.
- Fare clic su **Prefix Length** (Lunghezza prefisso) per specificare la lunghezza e immettere il numero di bit che costituiscono il prefisso dell'indirizzo IP di origine. L'intervallo valido è compreso tra 0 e 32.

Passaggio 6. Fare clic su **Apply** (Applica) per impostare il filtro dei frammenti IP in modo che venga scritto nel file di configurazione in esecuzione.