Configurazione del filtro di sincronizzazione (SYN) sugli switch gestiti serie 300

Obiettivo

Il protocollo TCP è un protocollo del livello trasporto che fornisce un recapito ordinato e affidabile dei pacchetti e consente inoltre il rilevamento degli errori e dei dati persi per attivare la ritrasmissione finché i dati non vengono ricevuti completamente e correttamente. Prima di inviare i dati, il client richiede una connessione con un pacchetto di sincronizzazione (SYN) al server per avviare la connessione. Il server invia quindi un pacchetto SYN e di conferma (ACK) al client, il quale invia un pacchetto ACK per confermare la risposta del server. Dopo questa connessione handshake a tre vie tra il client e il server, è possibile inviare i dati.

Un attacco di tipo SYN flood si verifica quando l'handshake TCP a tre vie viene interrotto. Un client dannoso inonda il server di pacchetti SYN, il server risponde con pacchetti SYN e ACK per tutte le richieste del client dannoso, ma il client dannoso non restituisce i pacchetti ACK. Il server attende un pacchetto ACK che non arriverà, il che consuma le risorse del server per gli utenti legittimi e alla fine disattiva la rete. Il filtro SYN previene questi attacchi. Questo articolo spiega come configurare il filtro SYN sugli switch gestiti serie 300.

Dispositivi interessati

·SF/SG serie 300 Managed Switch

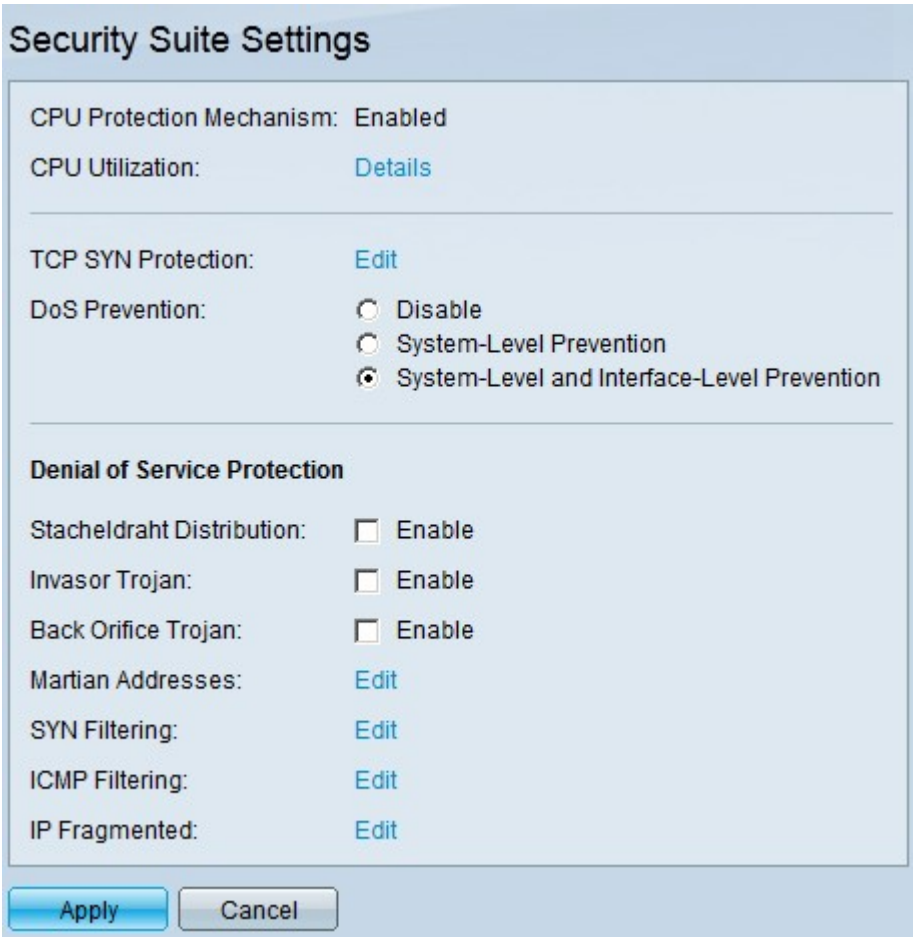
Versione del software

·v1.2.7.76

Abilita prevenzione del livello di negazione del servizio

Per applicare il filtro SYN, è necessario innanzitutto verificare che lo switch esegua correttamente la prevenzione del livello Denial of Service. Questa sezione spiega come abilitare il corretto livello di prevenzione sugli switch gestiti serie 300.

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*:



Passaggio 2. Nel campo della prevenzione DoS, esistono tre livelli di prevenzione. Fare clic su **Prevenzione a livello di sistema e di interfaccia**. Questo livello consente di configurare il filtro SYN.

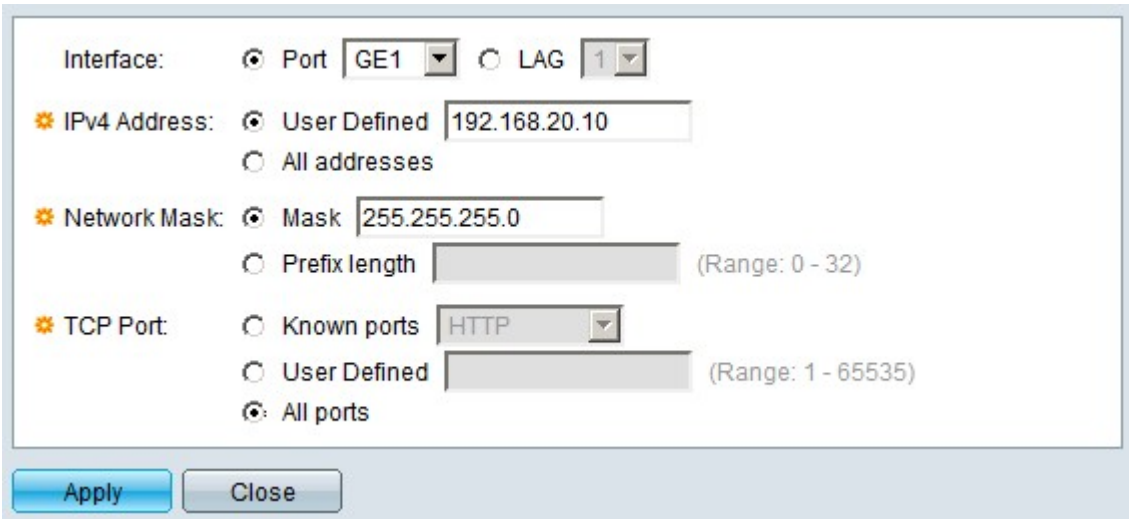
Passaggio 3. Fare clic su **Apply** per salvare la configurazione.

Filtra pacchetti TCP SYN

Questa sezione spiega come configurare il filtro SYN sugli switch gestiti serie 300.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Prevenzione della negazione del servizio > Filtro SYN**. Viene visualizzata la pagina *SYN Filtering* (Filtro SYN):

Passaggio 2. Fare clic su **Add**. Viene visualizzata la finestra *Aggiungi filtro SYN*:



Passaggio 3. Nel campo Interfaccia, fare clic sul pulsante di opzione di una delle opzioni di interfaccia disponibili:

·Port - Consente di scegliere la porta dalla quale filtrare i pacchetti SYN dall'elenco a discesa Port.

·LAG: consente di scegliere il LAG dal quale filtrare i pacchetti SYN dall'elenco a discesa Link Aggregation Group (LAG). Un LAG raggruppa più porte in un'unica porta logica.

Passaggio 4. Nel campo Indirizzo IPv4, fare clic sul pulsante di opzione di una delle opzioni disponibili per definire l'indirizzo o gli indirizzi IPv4 da cui filtrare i pacchetti SYN:

·Definito dall'utente: consente di immettere l'indirizzo IPv4 per il quale è definito il filtro dei pacchetti SYN.

·Tutti gli indirizzi: questa opzione filtra tutti gli indirizzi IPv4 per i pacchetti SYN.

5. Nel campo Network Mask (Maschera di rete), fare clic sul pulsante di opzione di una delle opzioni disponibili per immettere la maschera di rete dell'indirizzo IP configurato nel Step 4:

·Maschera — questa opzione consente di immettere la subnet mask dell'indirizzo IP.

·Lunghezza prefisso — questa opzione consente di immettere l'indirizzo IP della subnet mask nel formato del prefisso.

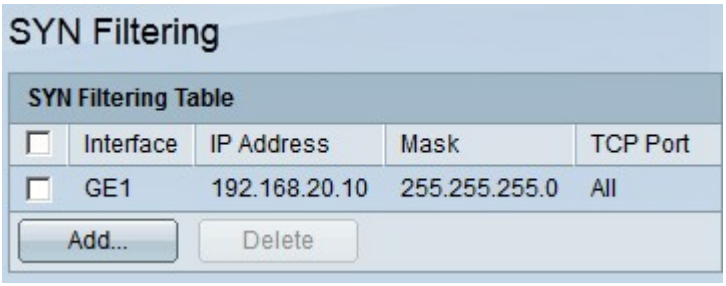
Passaggio 5. Nel campo Porta TCP, fare clic su una delle opzioni disponibili per determinare le porte TCP da filtrare:

·Porte conosciute: questa opzione consente di scegliere le porte dall'elenco a discesa Porte conosciute. Ad esempio, HTTP è 80 e TELNET è 23.

·Definita dall'utente - Questa opzione consente di immettere i numeri di porta TCP da filtrare.

·Tutte le porte - Questa opzione filtra tutte le porte TCP.

Passaggio 6. Fare clic su **Apply** (Applica) per salvare la configurazione. Le modifiche vengono apportate alla tabella del filtro SYN:



Passaggio 7. (Facoltativo) Per eliminare un filtro SYN, nella tabella dei filtri SYN, selezionare la casella di controllo del filtro SYN da eliminare. Quindi fare clic su **Elimina**.