

# Configurazione del filtro SYN Denial of Service (DoS) sugli switch gestiti serie 300

## Obiettivo

Un attacco Denial of Service (DoS) inonda una rete con traffico falso. In questo modo le risorse del server di rete vengono sottratte agli utenti legittimi. Un'inondazione SYN è destinata in particolare al protocollo TCP. Il protocollo TCP richiede tre passaggi per funzionare. In primo luogo, un utente invia il proprio indirizzo IP al server e richiede una connessione. Successivamente, il server risponde alla richiesta e attende una conferma. Infine, l'utente riconosce che il server ha aperto una connessione. Un attacco TCP SYN utilizza più indirizzi IP per richiedere una connessione, ma non invia mai una conferma al server una volta aperta una connessione. Un server può aprire solo una quantità limitata di connessioni prima di iniziare a eliminare le richieste TCP, anche da utenti legittimi.

Il traffico TCP viene inviato su diverse porte virtuali. Queste porte consentono di suddividere il traffico di rete in gruppi comuni. È possibile configurare il filtro SYN per bloccare il traffico proveniente da una porta virtuale specifica. Inoltre, il filtro SYN è configurato su una porta fisica o su un LAG effettivi sullo switch. Questo articolo spiega come configurare il filtro SYN sugli switch gestiti serie 300.

**Nota:** I filtri di sincronizzazione possono essere utilizzati solo se è abilitata la prevenzione DoS. Per ulteriori informazioni, fare riferimento all'articolo *Impostazioni della Security Suite sugli switch gestiti serie 300*.

## Dispositivi interessati

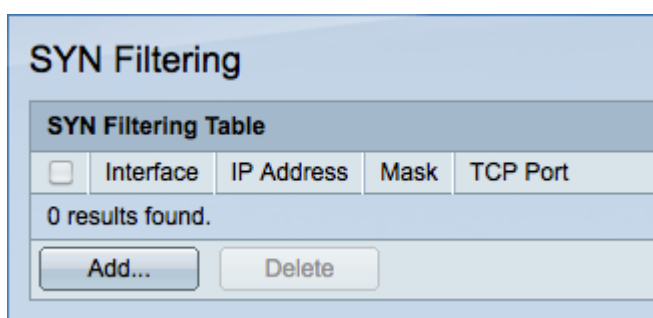
·SF/SG serie 300 Managed Switch

## Versione del software

·v1.2.7.76

## Configurazione filtro SYN

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):



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

Passaggio 2. Fare clic su **Add** per aggiungere un nuovo filtro SYN. Verrà visualizzata la

finestra *Aggiungi filtro di sincronizzazione*.

Interface:  Port GE1  LAG 1

IPv4 Address:  User Defined 192.0.2.10  
 All addresses

Network Mask:  Mask 255.255.255.0  
 Prefix length (Range: 0 - 32)

TCP Port:  Known ports HTTP  
 User Defined 8080 (Range: 1 - 65535)  
 All ports

Apply Close

Passaggio 3. Fare clic sul pulsante di opzione corrispondente all'interfaccia desiderata nel campo Interfaccia. Posizione fisica a cui verrà assegnato il filtro.

·Porta: la porta fisica sullo switch. Selezionare una porta specifica dall'elenco a discesa Porta.

·LAG: gruppo di porte che fungono da porta singola. Scegliere un LAG specifico dall'elenco a discesa LAG.

Passaggio 4. Fare clic sul pulsante di opzione corrispondente all'indirizzo IPv4 desiderato nel campo Indirizzo IPv4.

·Definito dall'utente: immettere un indirizzo IP da filtrare per il traffico TCP.

·Tutti gli indirizzi: tutti gli indirizzi IPv4 vengono filtrati in base al traffico TCP. Andare al passaggio 6 se è stato scelto Tutti gli indirizzi.

Passaggio 5. Fare clic sul pulsante di opzione corrispondente al metodo utilizzato per definire la subnet mask dell'indirizzo IP nel campo Network Mask.

·Maschera — immettere la maschera di rete nel campo Network mask.

·Lunghezza prefisso - immettere la lunghezza del prefisso (numero intero compreso tra 0 e 32) nel campo Lunghezza prefisso.

Passaggio 6. Fare clic sul pulsante di opzione corrispondente alla porta TCP desiderata da filtrare nel campo Porta TCP. Si tratta delle porte virtuali in cui è suddiviso il traffico di rete.

·Porte conosciute: scegliere una porta TCP da filtrare dall'elenco a discesa Porte conosciute.

·Definita dall'utente: immettere una porta TCP da filtrare.

·Tutte le porte: tutte le porte TCP vengono filtrate.

Passaggio 7. Fare clic su **Apply** per salvare le modifiche, quindi su **Close** (Chiudi) per uscire dalla finestra *Add Syn Filtering* (Aggiungi filtro sincrono).