Configurazione del filtro dei frammenti IP DoS (Denial of Service) sugli switch gestiti serie 300

Obiettivo

Il traffico di rete viene inviato utilizzando più pacchetti denominati datagrammi. Ogni metodo di trasporto (Ethernet, token ring, ecc.) ha una dimensione massima di datagramma che può gestire. Se il datagramma è troppo grande per il metodo di trasmissione, viene suddiviso in frammenti più piccoli. Questo processo è noto come frammentazione IP. La maggior parte del traffico di rete non deve essere frammentata. Infatti, il traffico che è stato frammentato può essere usato come in un attacco Denial of Service (DoS). Un attacco DoS inonda una rete con traffico falso e rallenta o arresta la rete. Gli switch gestiti serie 300 possono bloccare i frammenti IP, riducendo la vulnerabilità della rete a un attacco DoS. In questo documento viene spiegato come configurare le impostazioni del *filtro dei frammenti IP* sugli switch gestiti serie 300.

Nota: I filtri dei frammenti IP 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

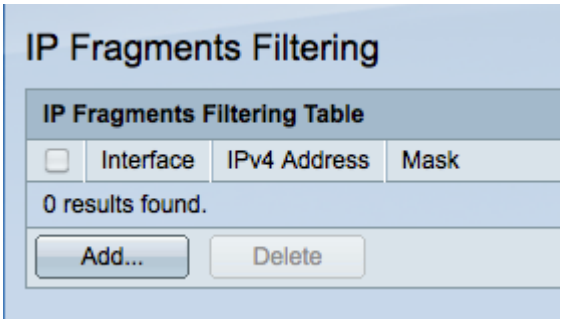
·SF/SG serie 300 Managed Switch

Versione del software

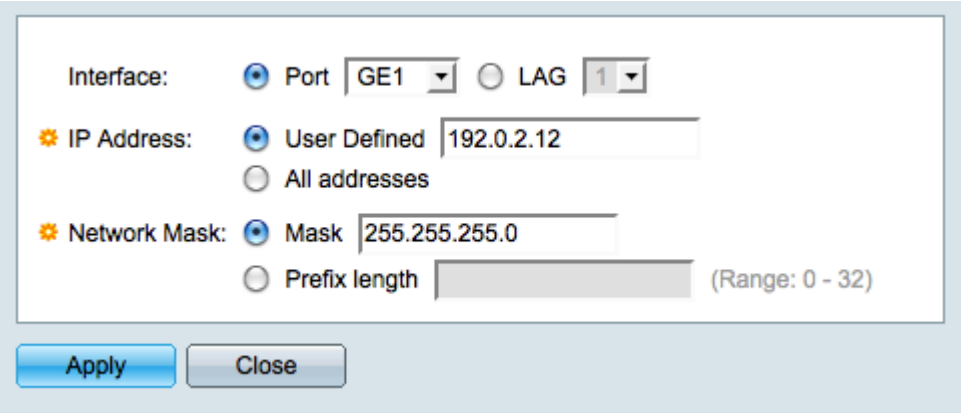
•1.3.0.62

Aggiungi filtro frammenti IP

Passaggio 1. Accedere all'utility di configurazione Web e selezionare **Security > Denial Of Service Prevention > IP Fragments Filtering (Sicurezza > Prevenzione della negazione del servizio > Filtro frammenti IP).** Viene visualizzata la pagina *IP Fragments Filtering* (Filtro frammenti IP):



Passaggio 2. Fare clic su **Add** (Aggiungi) per aggiungere un nuovo filtro ai frammenti IP. Viene visualizzata la finestra *Add IP Fragments Filtering* (Aggiungi filtro frammenti IP).



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 da filtrare nel campo Indirizzo IP.

·Definito dall'utente: immettere un indirizzo IP da filtrare.

·Tutti gli indirizzi: tutti gli indirizzi IPv4 vengono filtrati.

Nota: Se si sceglie Tutti gli indirizzi al passaggio 4, andare al passaggio 6.

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 su **Apply** per salvare le modifiche, quindi su **Close** (Chiudi) per chiudere la finestra *Add IP Fragments Filtering* (Aggiungi filtro frammenti IP).