Configurazione del filtro dei frammenti IP DoS (Denial of Service) sugli switch serie Sx500 impilabili

Obiettivo

La prevenzione DoS (Denial of Service) aumenta la sicurezza della rete e filtra i pacchetti con determinati parametri di indirizzo IP in modo che non entrino nella rete. Per impostazione predefinita, le dimensioni massime del pacchetto IP sono di 1500 byte, ma quando il pacchetto supera tali dimensioni il pacchetto deve essere frammentato. Questi pacchetti devono essere bloccati a volte perché possono presentare alcune vulnerabilità della sicurezza. È possibile, ad esempio, creare troppi datagrammi incompleti per causare la negazione del servizio e tentare di ignorare le misure di sicurezza.

Il filtro dei frammenti IP DoS viene usato per bloccare i pacchetti IP frammentati. Questo documento spiega come configurare le impostazioni di filtro dei frammenti IP DoS sugli switch impilabili serie Sx500.

Dispositivi interessati

·Switch Stack Serie Sx500

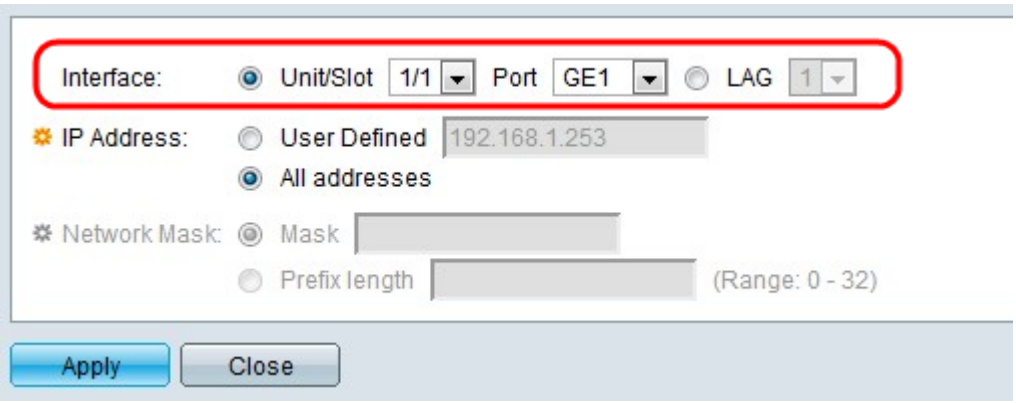
Versione del software

·v1.2.7.76

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. Nella tabella del filtro dei frammenti IP, fare clic su **Add** (Aggiungi). Viene visualizzata la finestra *Add IP Fragments Filtering* (Aggiungi filtro frammenti IP).

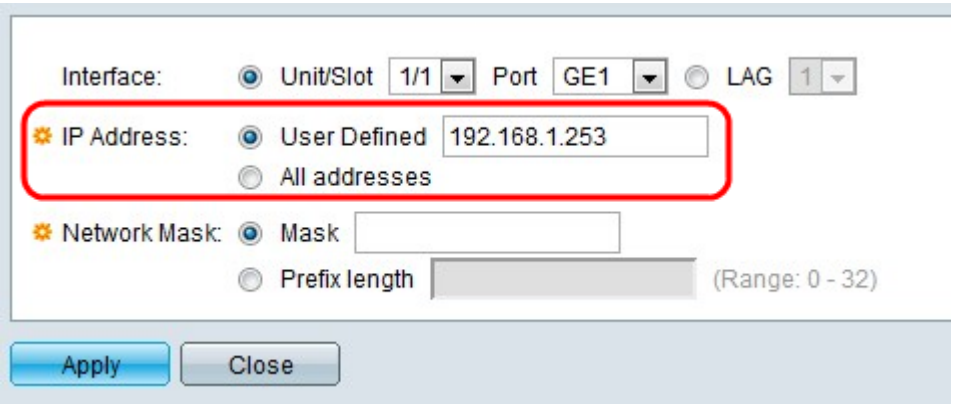


Passaggio 3. Fare clic sul pulsante di opzione corrispondente al tipo di interfaccia desiderato nel campo Interfaccia.

·Unità/Slot: dagli elenchi a discesa Unità/Slot scegliere l'Unità/Slot appropriato. L'unità identifica se lo switch è attivo o è un membro dello stack. Lo slot identifica lo switch collegato a quale slot (lo slot 1 è SF500 e lo slot 2 è SG500). Se non conosci i termini usati, controlla Cisco Business: glossario dei nuovi termini.

- Porta: dall'elenco a discesa Porta, scegliere la porta appropriata da configurare.

·LAG - Scegliere il LAG desiderato dall'elenco a discesa LAG. Un LAG (Link Aggregate Group) viene utilizzato per collegare più porte. I LAG moltiplicano la larghezza di banda, aumentano la flessibilità delle porte e forniscono la ridondanza dei collegamenti tra due dispositivi per ottimizzare l'utilizzo delle porte.

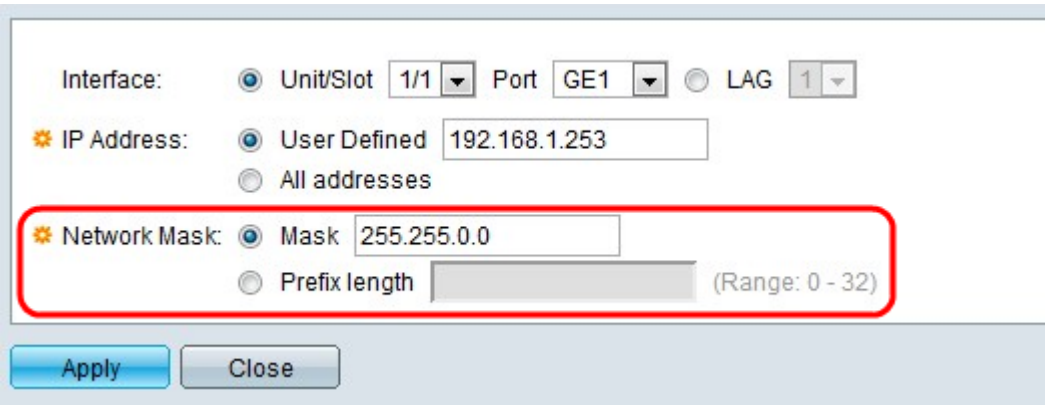


Passaggio 4. Fare clic sul pulsante di opzione corrispondente all'indirizzo IP da cui i pacchetti devono essere filtrati nel campo Indirizzo IP.

·Definito dall'utente: immettere un indirizzo IP da cui filtrare i pacchetti IP frammentati.

·Tutti gli indirizzi: blocca i pacchetti IP frammentati da tutti gli indirizzi.

Nota: Se nel passaggio 4 si è scelto Tutti gli indirizzi, andare al passaggio 6.



Passaggio 5. Fare clic sul pulsante di opzione corrispondente alla network mask desiderata nel campo Network Mask.

·Maschera — immettere la maschera di rete in formato indirizzo IP. Definisce la subnet mask dell'indirizzo IP.

·Lunghezza prefisso — immettere la lunghezza del prefisso (numero intero compreso tra 0 e 32). La subnet mask viene definita in base alla lunghezza del prefisso dell'indirizzo IP.

Passaggio 6. Fare clic su **Applica**.