Configuración de filtrado de fragmentos de IP de denegación de servicio (DoS) en switches apilables de la serie Sx500

Objetivo

La prevención de denegación de servicio (DoS) aumenta la seguridad de la red y filtra los paquetes con determinados parámetros de dirección IP para que no entren en la red. El tamaño máximo del paquete IP es 1500 bytes de forma predeterminada, pero cuando el paquete excede este tamaño, el paquete necesita fragmentarse. Estos paquetes necesitan ser bloqueados a veces porque pueden plantear algunas vulnerabilidades de seguridad, como que se puedan crear demasiados datagramas incompletos para causar la denegación de servicio y pueden intentar eludir las medidas de seguridad.

El filtrado de fragmentos IP de DoS se utiliza para bloquear los paquetes IP fragmentados. Este documento explica cómo configurar la configuración de filtrado de fragmentos IP de DoS en los switches apilables de la serie Sx500.

Dispositivos aplicables

Switches apilables · Sx500 Series

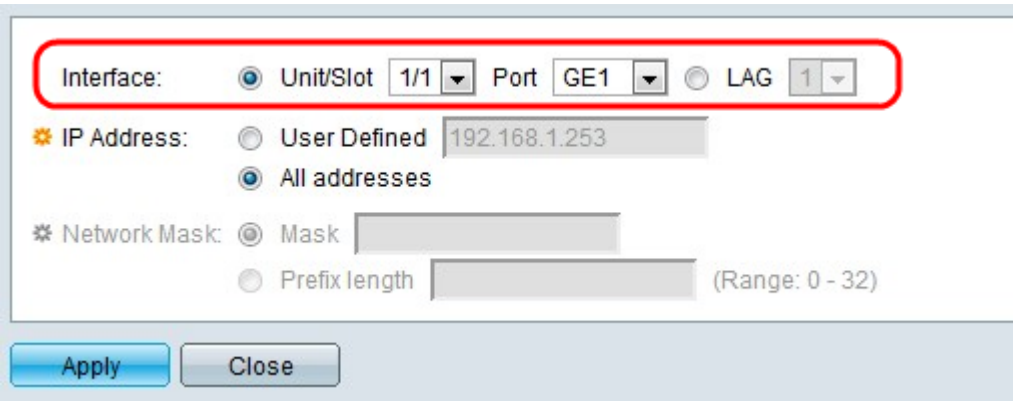
Versión del software

•v1.2.7.76

Agregar filtro de tramas IP

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > Denial Of Service Prevention > IP Fragments Filtering .** Se abre la página *Filtrado de Fragmentos IP*:

Paso 2. En la Tabla de Filtrado de Fragmentos IP, haga clic en **Agregar**. Aparece la ventana *Add IP Fragments Filtering*.

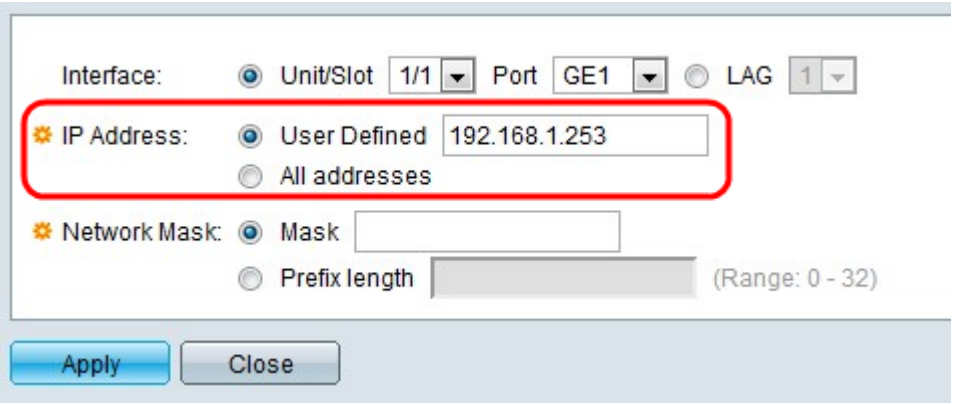


Paso 3. Haga clic en el botón de opción correspondiente al tipo de interfaz deseado en el campo Interface (Interfaz).

·Unidad/Ranura: en las listas desplegables Unidad/Ranura elija la unidad/Ranura adecuada. La unidad identifica si el switch está activo o si es miembro de la pila. La ranura identifica qué switch está conectado a qué ranura (la ranura 1 es SF500 y la ranura 2 es SG500). Si no conoce los términos utilizados, consulte Cisco Business: Glosario de nuevos términos.

- Puerto: en la lista desplegable Puerto, elija el puerto apropiado para configurar.

·LAG: elija el LAG deseado en la lista desplegable LAG. Se utiliza un grupo de agregación de enlaces (LAG) para vincular varios puertos entre sí. Los LAG multiplican el ancho de banda, aumentan la flexibilidad de los puertos y proporcionan redundancia de link entre dos dispositivos para optimizar el uso de los puertos.

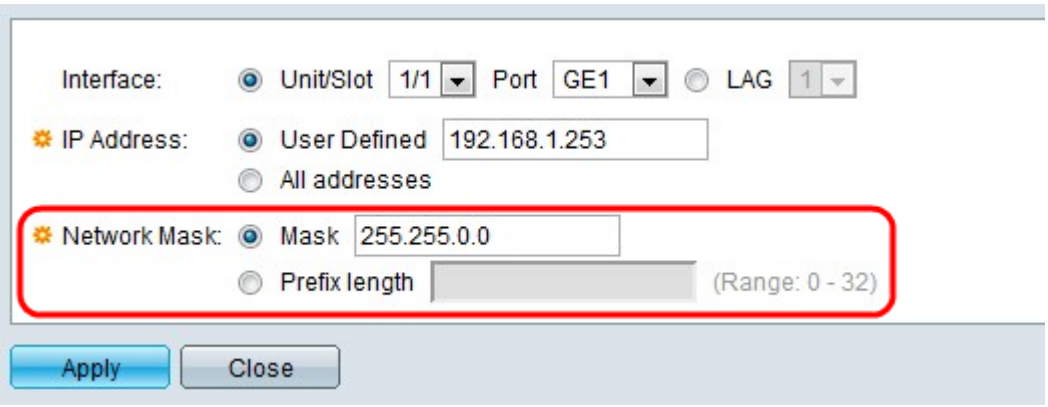


Paso 4. Haga clic en el botón de opción correspondiente a la dirección IP desde la que se filtrarán los paquetes en el campo IP Address (Dirección IP).

·definido por el usuario: introduzca una dirección IP desde la que se filtren los paquetes IP fragmentados.

·Todas las direcciones: bloquea los paquetes IP fragmentados de todas las direcciones.

Nota: Si selecciona Todas las direcciones en el paso 4, vaya al paso 6.



Paso 5. Haga clic en el botón de opción correspondiente a la máscara de red deseada en el campo Máscara de red.

Máscara de ·: introduzca la máscara de red en el formato de dirección IP. Esto define la máscara de subred para la dirección IP.

·longitud del prefijo: introduzca la longitud del prefijo (entero en el rango de 0 a 32). Esto define la máscara de subred por longitud de prefijo para la dirección IP.

Paso 6. Haga clic en Apply (Aplicar).