Configuración de técnicas de prevención de denegación de servicio (Security Suite) en switches apilables de la serie Sx500

Objetivo

Los ataques de denegación de servicio (DoS) o de denegación de servicio distribuida (DDoS) restringen el uso de la red por parte de los usuarios válidos. El atacante realiza un ataque DOS inundando una red con muchas solicitudes innecesarias que ocupan todo el ancho de banda de la red. Los ataques DoS pueden ralentizar una red o desconectar completamente una red durante varias horas. La protección DoS es la función principal para mejorar la seguridad de la red; detecta el tráfico anormal y lo filtra.

En este artículo se explica la configuración de la denegación de servicio en la configuración de la suite de seguridad y varias técnicas utilizadas para la prevención de denegación de servicio.

Nota: Si la prevención de DoS elegida es de nivel de sistema y prevención de nivel de interfaz, se pueden editar y configurar las direcciones marciales, el filtrado SYN, la protección de velocidad SYN, el filtrado ICMP y el filtrado de fragmentos IP. Estas configuraciones también se explican en este artículo.

Nota: Antes de activar la prevención de DoS, es necesario desenlazar todas las listas de control de acceso (ACL) o cualquier política de QoS avanzada configurada en el puerto. Las políticas de ACL y QoS avanzadas no están activas una vez que la protección de DoS está habilitada en el puerto.

Dispositivos aplicables

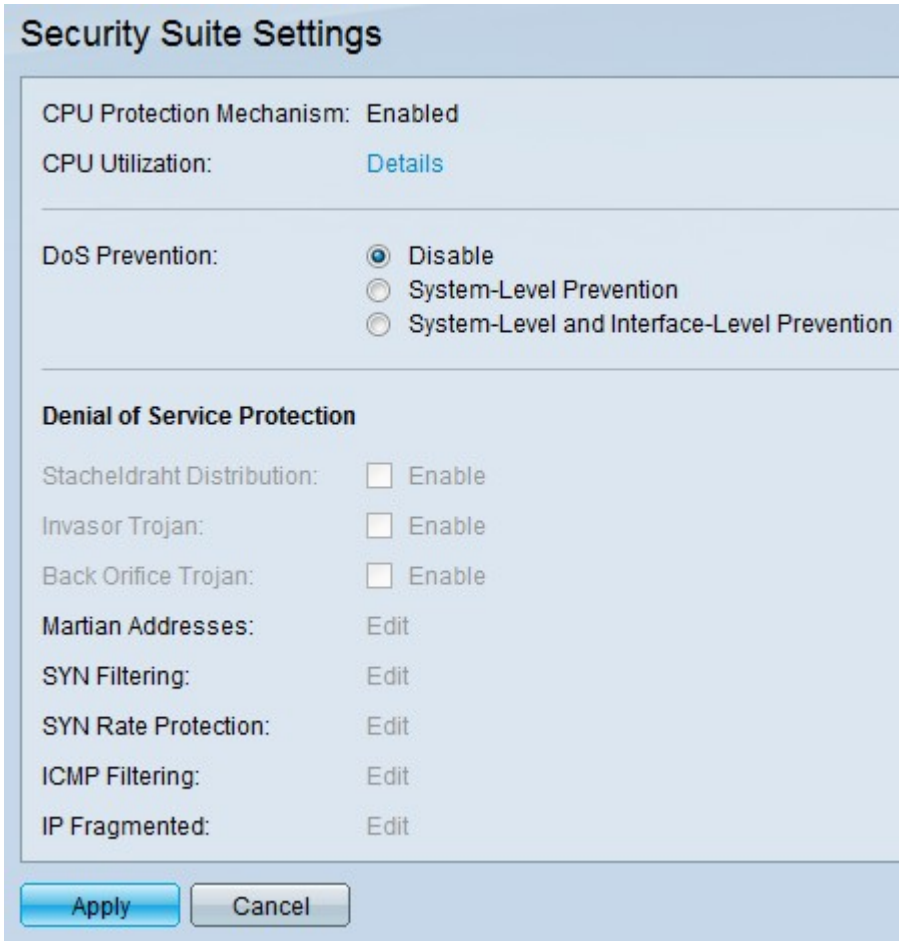
- Switches apilables serie Sx500

Versión del software

- 1.3.0.62

Configuración de la denegación de servicio en la configuración del conjunto de aplicaciones de seguridad

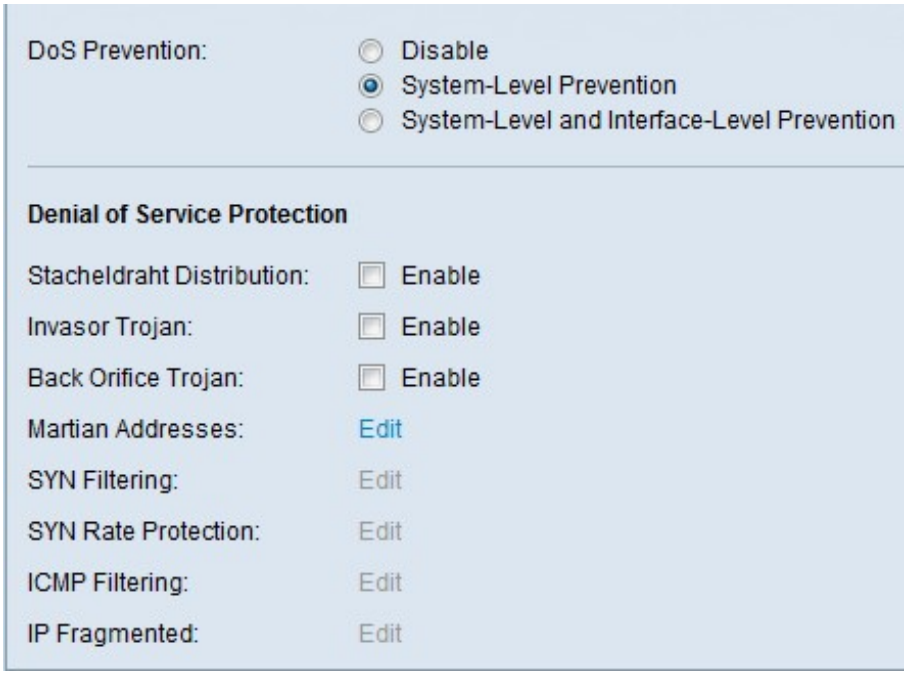
Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > Denial of Service Prevention > Security Suite Settings**. Se abre la página *Configuración del conjunto de seguridad*:



- Mecanismo de protección de la CPU: esto es
- **Habilitado.** Esto indica que la herramienta de conversión de seguridad (SCT) está activada.
- Utilización de la CPU: haga clic en
- **Detalles** junto a la utilización de la CPU para ver la información de utilización de recursos de la CPU.

Paso 2. Haga clic en el botón de opción correspondiente en el campo DoS Prevention (Prevención de DoS).

- Desactivar: para desactivar la prevención de DoS.
- Prevención a nivel del sistema: esto evita los ataques de Stacheldraht Distribution, troyano Invasor y troyano de Back Orifice.
- Prevención de nivel de sistema e interfaz: esto evita ataques por interfaz en el switch.



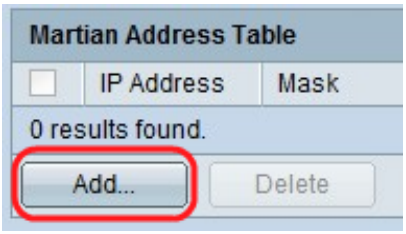
Paso 3. Estas opciones se pueden elegir para la protección de denegación de servicio:

- Distribución de Stacheldraht: Este es un ejemplo de ataque DDoS donde el atacante utiliza un programa cliente para conectarse a los equipos dentro de la red. A continuación, esos ordenadores envían varias solicitudes de inicio de sesión al servidor interno e inician un ataque DDoS.
- Troyano Invasor: si el equipo está infectado por este ataque, el puerto TCP 2140 se utiliza para la actividad maliciosa. .
- Troyano de Back Orifice: Descarta los paquetes UDP que se utilizan para comunicarse con el servidor y el programa cliente para el ataque de DoS.

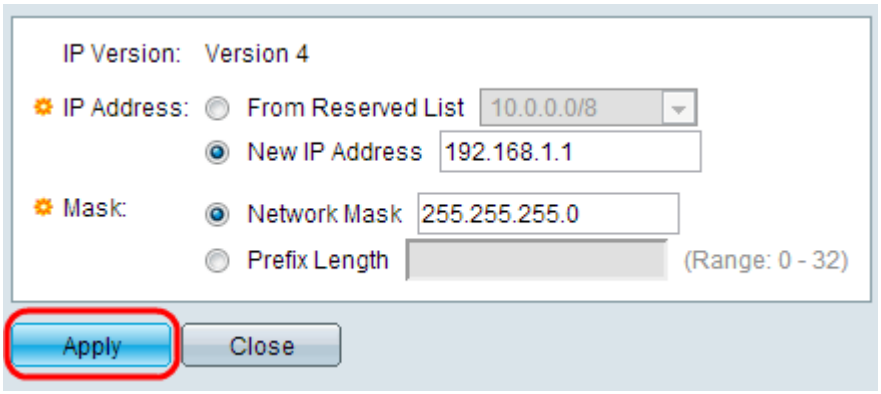
Configuración de las Direcciones Marcianas

Paso 1. Haga clic en **Editar** en el campo Direcciones marcianas y, a continuación, se abrirá la página *Direcciones marcianas*. Las direcciones marcianas indican la dirección IP que puede ser la causa de un ataque en la red. Los paquetes que vienen de estas redes se descartan.

Paso 2. Marque **Incluir** en las direcciones marcianas reservadas y haga clic en **Aplicar** para agregar las direcciones marcianas reservadas en la lista Prevención de nivel del sistema.



Paso 3. Para agregar una dirección marciana, haga clic en **Agregar**. Se muestra la página *Agregar direcciones marcianas*. Introduzca estos parámetros:



Paso 4. En el campo IP Address (Dirección IP), introduzca la dirección IP que debe rechazarse.

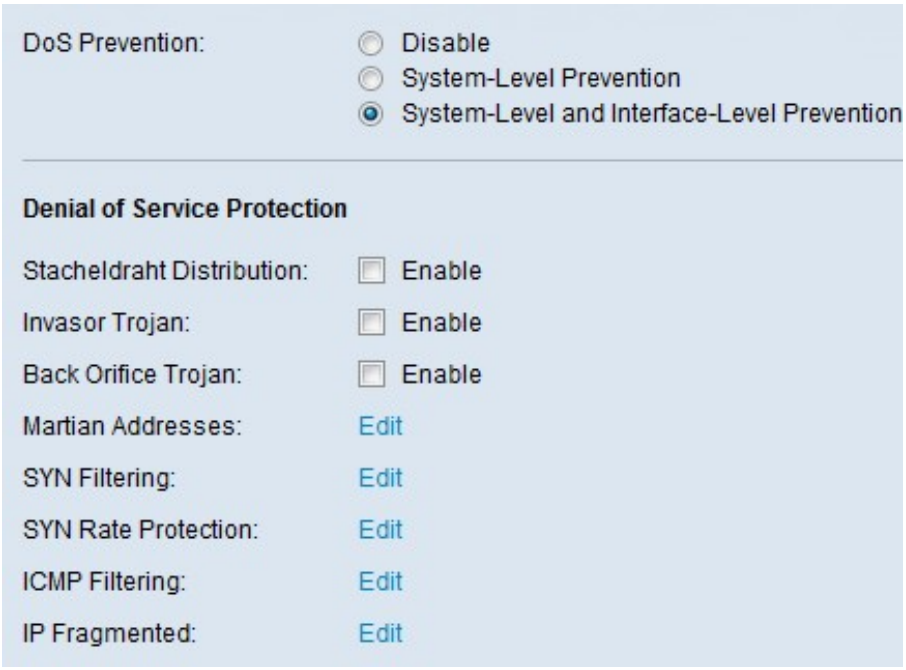
Paso 5. La máscara de dirección IP para indicar el rango de direcciones IP que deben rechazarse.

- Versión IP: la versión IP admitida. Actualmente, sólo se permite IPv4.
- De la lista reservada: elija una dirección IP conocida de la lista reservada.
- Nueva dirección IP: introduzca una dirección IP.
- Máscara de red: Máscara de red con el formato decimal punteado.
- Longitud del prefijo: Prefijo de la dirección IP para definir el rango de direcciones IP para el que está habilitada la prevención de denegación de servicio.

Paso 6. Haga clic en **Aplicar** para que la dirección marciana se escriba en el archivo Configuración en ejecución.

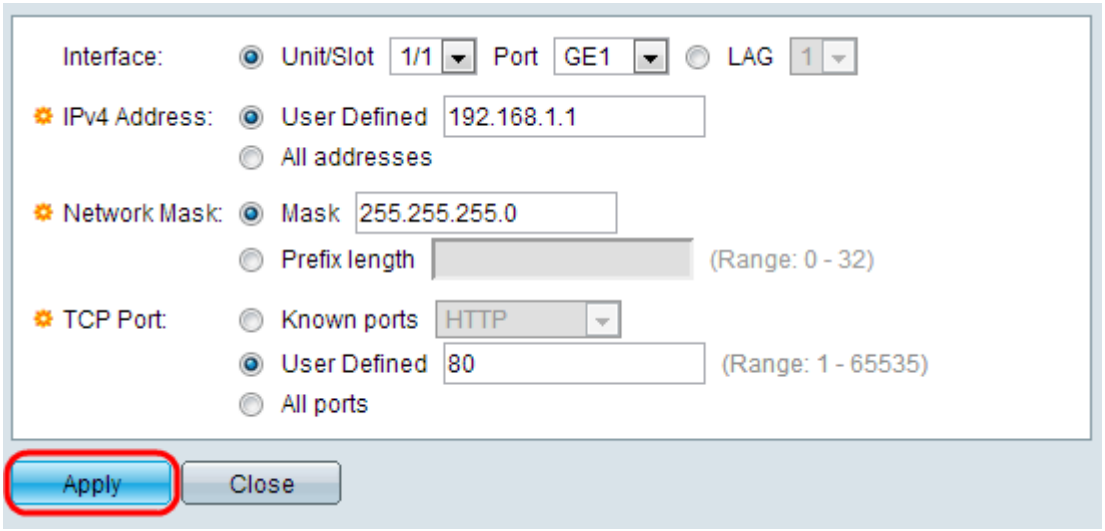
Configuración del Filtrado SYN

El filtrado SYN permite a los administradores de red descartar paquetes TCP ilegales con el indicador SYN. El filtrado de puertos SYN se define por puerto.



Paso 1. Para configurar el filtrado SYN, haga clic en **Editar** y se abrirá la *página Filtrado SYN*:

Paso 2. Haga clic en Add (Agregar). Se muestra la página *Agregar filtrado SYN*. Introduzca estos parámetros en los campos mostrados:

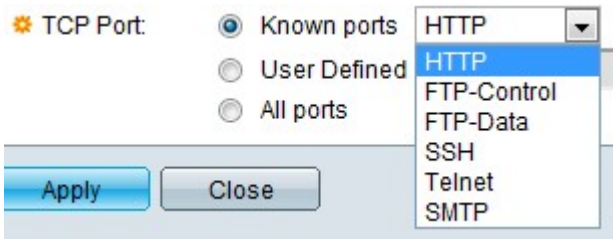


Paso 3. Elija la interfaz en la que se debe definir el filtro.

Paso 4. Haga clic en **User Defined** para dar una dirección IP para la que se define el filtro o haga clic en **All Addresses**.

Paso 5. La máscara de red para la que está habilitado el filtro. Haga clic en **Longitud del prefijo** para especificar la longitud, su rango está entre 0 y 32, o haga clic en **Máscara** para

ingresar la máscara de subred como en la notación decimal con puntos.



Paso 6. Haga clic en el puerto TCP de destino que se está filtrando. Son de los tipos siguientes:

- Puertos conocidos: elija un puerto de la lista.
- Definido por el usuario: introduzca el número de puerto.
- Todos los puertos: haga clic para indicar que se filtran todos los puertos.

Paso 7. Haga clic en **Aplicar** para que el filtrado SYN se escriba en el archivo de configuración en ejecución.

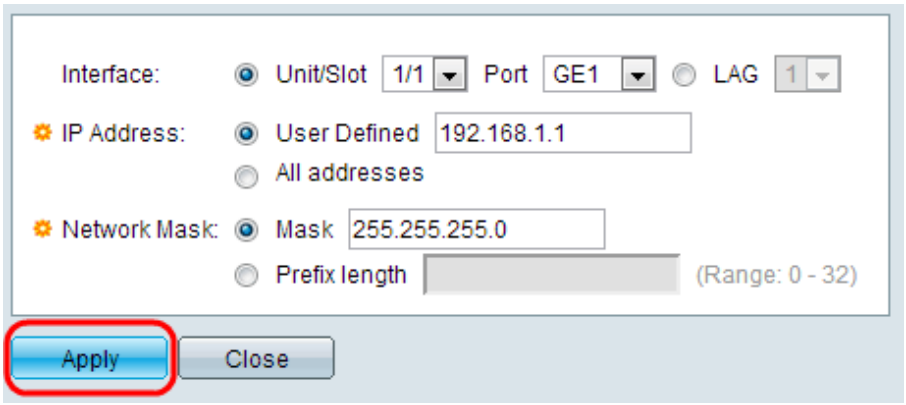
Configuración del Filtrado ICMP

El protocolo de mensajes de control de Internet (ICMP) es uno de los protocolos de Internet más importantes. Es un protocolo de capa de red. Los sistemas operativos utilizan ICMP para enviar mensajes de error que indican que el servicio solicitado no está disponible o que no se puede alcanzar un host determinado. También se utiliza para enviar mensajes de diagnóstico. El ICMP no se puede utilizar para intercambiar datos entre los sistemas. Normalmente se generan en respuesta a algunos errores en los datagramas IP.

El tráfico ICMP es un tráfico de red muy importante, pero también puede provocar muchos problemas de red si un atacante malintencionado lo utiliza contra la red. Esto plantea la necesidad de filtrar estrictamente el tráfico ICMP que viene de Internet. La página *Filtrado ICMP* habilita el filtrado de los paquetes ICMP de orígenes específicos. Esto minimiza la carga en la red en caso de que haya algún ataque ICMP.

Paso 1. Para configurar el filtrado ICMP, haga clic en **Editar** y se abrirá la página *Filtrado ICMP*.

Paso 2. Haga clic en Add (Agregar). Se muestra la página *Add ICMP Filtering* . Introduzca estos parámetros en los campos mostrados:



Paso 3. Elija la interfaz en la que se define el Filtrado ICMP.

Paso 4. Ingrese la dirección IPv4 para la que está habilitado el filtrado de paquetes ICMP o haga clic en **Todas las direcciones** para bloquear los paquetes ICMP de todas las direcciones de origen. Si se introduce la dirección IP, introduzca la máscara o la longitud del prefijo.

Paso 5. La máscara de red para la que se habilita la protección de velocidad. Elija el formato de la máscara de red para la dirección IP de origen y haga clic en uno de los campos.

- Mask: elija la subred a la que pertenece la dirección IP de origen e introduzca la máscara de subred en formato decimal con puntos.
- Haga clic en **Longitud del prefijo** para especificar la longitud e introducir el número de bits que consta del prefijo de la dirección IP de origen, su rango está entre 0 y 32.

Paso 6. Haga clic en **Aplicar** para que el filtrado ICMP se escriba en el archivo de configuración en ejecución.

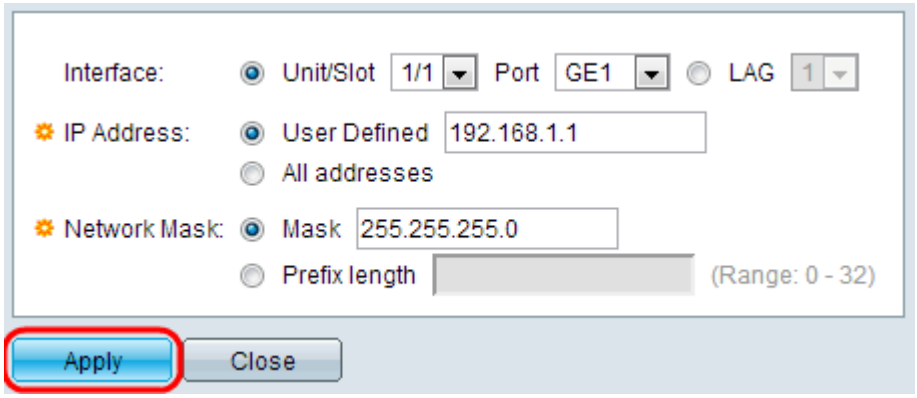
Configuración del Filtrado de Fragmentos IP

Todos los paquetes tienen un tamaño de unidad de transmisión máxima (MTU). MTU es el tamaño del paquete más grande que puede transmitir una red. IP aprovecha la fragmentación para que se puedan formar paquetes que puedan atravesar a través de un link con una MTU más pequeña que el tamaño del paquete original. Por lo tanto, los paquetes cuyos tamaños son mayores que la MTU permisible del link deben dividirse en paquetes más pequeños para permitirles atravesar el link.

Por otra parte, la fragmentación también puede plantear muchos problemas de seguridad. Por lo tanto, se hace necesario bloquear los fragmentos IP, ya que a veces pueden ser una razón para poner en peligro el sistema.

Paso 1. Para configurar el filtrado de fragmentos IP, haga clic en **Editar** y se abrirá la *página Filtrado de Fragmentos ICMP*.

Paso 2. Haga clic en Add (Agregar). Se muestra la página *Agregar filtrado de fragmentos de IP*. Introduzca estos parámetros en los campos mostrados:



Paso 3. Interfaz: Elija la interfaz en la que se define la fragmentación IP.

Paso 4. Dirección IP: introduzca la dirección IP para la que está habilitada la fragmentación IP o haga clic en **Todas las direcciones** para bloquear los paquetes IP fragmentados de todas las direcciones de origen. Si se introduce la dirección IP, introduzca la máscara o la longitud del prefijo.

Paso 5. Máscara de red: Máscara de red para la que se bloquea la fragmentación IP. Elija el formato de la máscara de red para la dirección IP de origen y haga clic en uno de los campos.

- Mask: elija la subred a la que pertenece la dirección IP de origen e introduzca la máscara de subred en formato decimal con puntos.
- Haga clic en **Longitud del prefijo** para especificar la longitud e introducir el número de bits que consta del prefijo de la dirección IP de origen, su rango está entre 0 y 32.

Paso 6. Haga clic en **Aplicar** para que el filtrado de fragmentos de IP se escriba en el archivo de configuración en ejecución.