Configuraciones de la habitación de la Seguridad en el Switches manejado 300 Series

Objetivo

La habitación de la Seguridad en el Switches manejado las Cisco 300 Series ofrece la protección contra los ataques de la negación de servicio (DOS). Los ataques DOS inundan las redes con el tráfico falso, que hace los recursos del servidor de red inasequibles o insensibles a los usuarios legítimos. Generalmente, hay dos tipos de ataques DOS. Los ataques DOS de la fuerza bruta inundan el servidor y consumen el servidor y el ancho de banda de la red. Los ataques sistemáticos manipulan las vulnerabilidades de los protocolos como el mensaje TCP SYN para bloquear los sistemas. Este artículo explica las configuraciones disponibles en la habitación de la Seguridad en el Switches manejado las 300 Series.

Nota: El Listas de control de acceso (ACL) y las directivas avanzadas de QoS no son activos en un puerto cuando se habilita la protección del ataque DOS.

Dispositivos aplicables

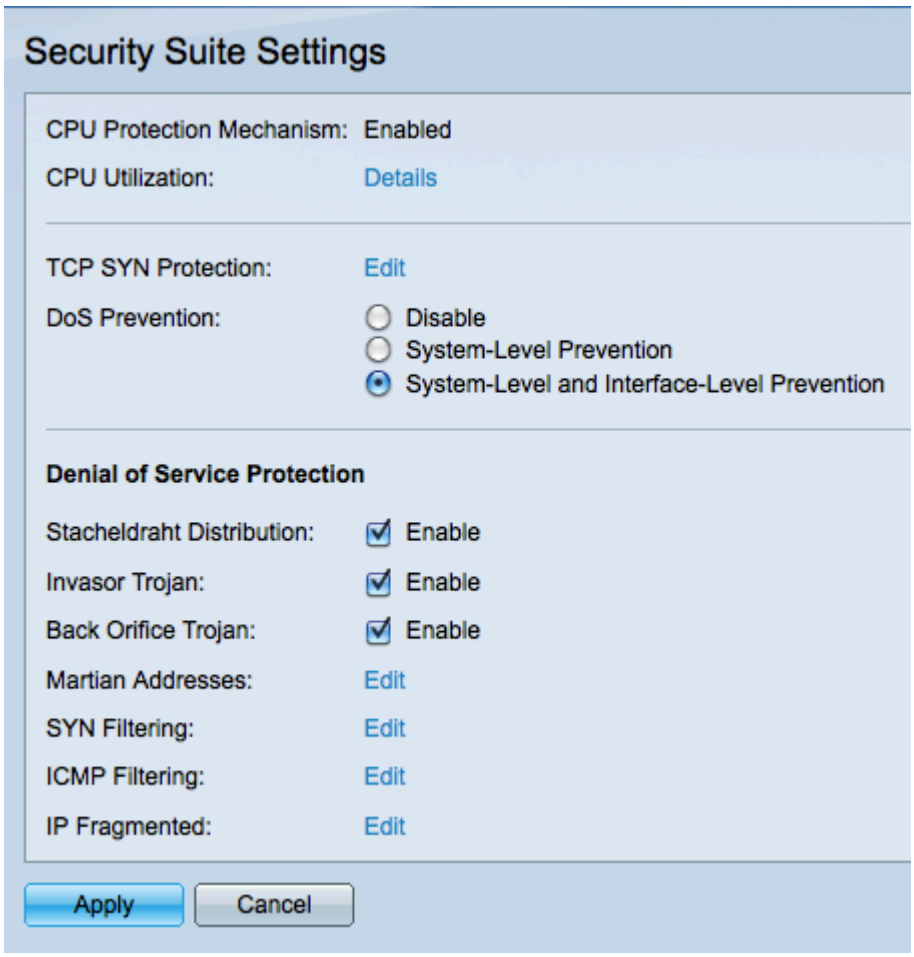
- Switches manejado 300 Series SF/SG

Versión del software

- 1.3.0.62

Configuración de las configuraciones de la habitación de la Seguridad

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija las **configuraciones de la habitación del > Security (Seguridad) de la prevención de la Seguridad > de la negación de servicio**. *La página Configuración de la habitación de la Seguridad* se abre:



Nota: El mecanismo de protección CPU se habilita por abandono en el Switches manejado las 300 Series y no puede ser inhabilitado. El Switch utiliza la tecnología de base segura (SCT), que permite que el Switch maneje la Administración y el tráfico de protocolo no importa cómo se recibe mucho tráfico total.

Los detalles (opcionales) del tecleo del paso 2. en la utilización de la CPU colocan para ver la utilización de la CPU. Refiera a la *utilización de la CPU del* artículo *en el Switches manejado las 200/300 Series* para más información.

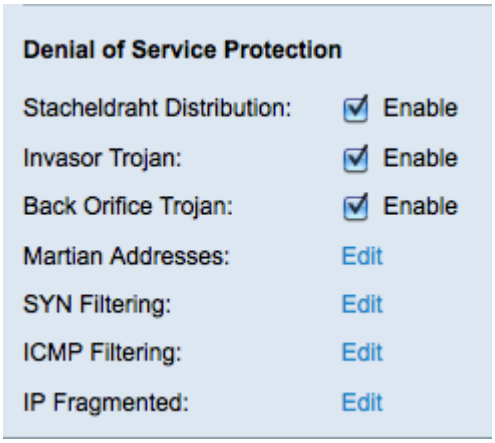
El tecleo (opcional) del paso 3. **edita** en el campo de la protección TCP SYN para editar las configuraciones de la protección TCP SYN. Refiera al artículo *sincronizan (SYN) la configuración de filtración en el Switches manejado las 300 Series* para más información.

Paso 4. En el campo de la prevención DOS, haga clic el botón de radio que corresponde al método de prevención DOS que usted quisiera emplear. Las opciones disponibles son:

- Neutralización — Característica de protección DoS de la neutralización. Si se elige la neutralización, salte al paso 13.

- Sistema - Nivel-prevención — Habilita las características de protección DoS que protegen contra el troyano de Invasor, la distribución de Stacheldraht, el troyano de Back Orifice, y los direccionamientos de Martian.

- Sistema - Protección de la Nivel-prevención y del Interfaz-nivel — Habilita todas las medidas de seguridad definidas en el área de la protección de la negación de servicio.



Paso 5. Marque la casilla de verificación del **permiso** en el campo de la distribución de Stacheldraht para desechar los paquetes TCP con un número del puerto TCP de la fuente de 16660.

Paso 6. Marque la casilla de verificación del **permiso** en el campo troyano de Invasor para desechar los paquetes TCP con un puerto del TCP de destino de 2140 y un puerto TCP de la fuente de 1024.

Paso 7. Marque la casilla de verificación del **permiso** en el campo troyano de Back Orifice para desechar los paquetes UDP con un puerto del destino UDP igual a 31337 y un puerto de la fuente UDP de 1024.

Nota: Mientras que hay centenares de ataques DOS, los puertos mencionados anteriormente se explotan comúnmente para la actividad maliciosa. Sin embargo, también se utilizan para el tráfico legítimo también. Si usted tiene un dispositivo que utilice un de los sobre los puertos, esa información será bloqueada.

Paso 8. El tecleo **edita** en el campo de direccionamientos marciano para editar la tabla de direccionamientos marciana. La tabla de direccionamientos marciana desecha los paquetes de los IP Addresses selectos. Para editar la lista de direccionamientos de Martian, refiera a la *configuración marciana del direccionamiento de la negación de servicio del* artículo *(DOS) en el Switches manejado las 300 Series*.

Nota: Los pasos 9-12 requieren a nivel sistema y la prevención del Interfaz-nivel se elija en el salto del paso 4. al paso 13 si usted ha elegido otro tipo de la prevención DOS.

Paso 9. El tecleo **edita** en el campo de filtración SYN para permitir que el administrador bloquee ciertos puertos TCP. Para configurar el SYN que filtra, refiera a la *configuración de filtración de la negación de servicio del* artículo *(DOS) SYN en el Switches manejado las 300 Series.*

Paso 10. El tecleo **edita** en el campo de la protección de la tarifa SYN para limitar el número de paquetes SYN recibidos. Para configurar la protección de la tarifa SYN, refiera a la *protección de la tarifa del* artículo *SYN en el Switches manejado las 300 Series*.

Paso 11 El tecleo **edita** en el campo del filtrado de ICMP para permitir que los paquetes icmp de ciertas fuentes sean bloqueados. Para configurar el filtrado de ICMP, refiera a la *configuración de filtración del Internet Control Message Protocol (ICMP) del* artículo *en el Switches manejado las 300 Series.*

Paso 12. El tecleo **edita** en el campo hecho fragmentos IP para bloquear los paquetes del IP hechos fragmentos. Para configurar los fragmentos IP que filtran, refiera a la *configuración*

de filtración de los fragmentos IP de la negación de servicio del artículo *(DOS) en el Switches manejado las 300 Series*.

Paso 13. El tecleo **se aplica** para salvar los cambios o la **cancelación del** tecleo para cancelar sus cambios.