Configuración y examen del proxy SOCKS en un dispositivo web seguro

Contenido

Introducción

Este documento describe cómo funciona el proxy SOCKS en Cisco SWA y proporciona una descripción general de cómo rutea el tráfico entre un cliente y el servidor final

Cómo funciona el proxy SOCKS en un nivel superior

Socket Secure (SOCKS) es un protocolo de red que facilita la comunicación con los servidores a través de un proxy SOCKS (en este caso, es SWA/WSA) mediante el enrutamiento del tráfico de red al servidor real en nombre de un cliente. SOCKS está diseñado para enrutar cualquier tipo de tráfico de capa de aplicación generado por cualquier programa.
El SWA utiliza de forma predeterminada el puerto TCP 1080 para escuchar el tráfico SOCKS del cliente. Los clientes pueden configurar para enviar el tráfico socks a WSA en el puerto TCP 1080. Si es necesario, puede agregar números de puerto adicionales.

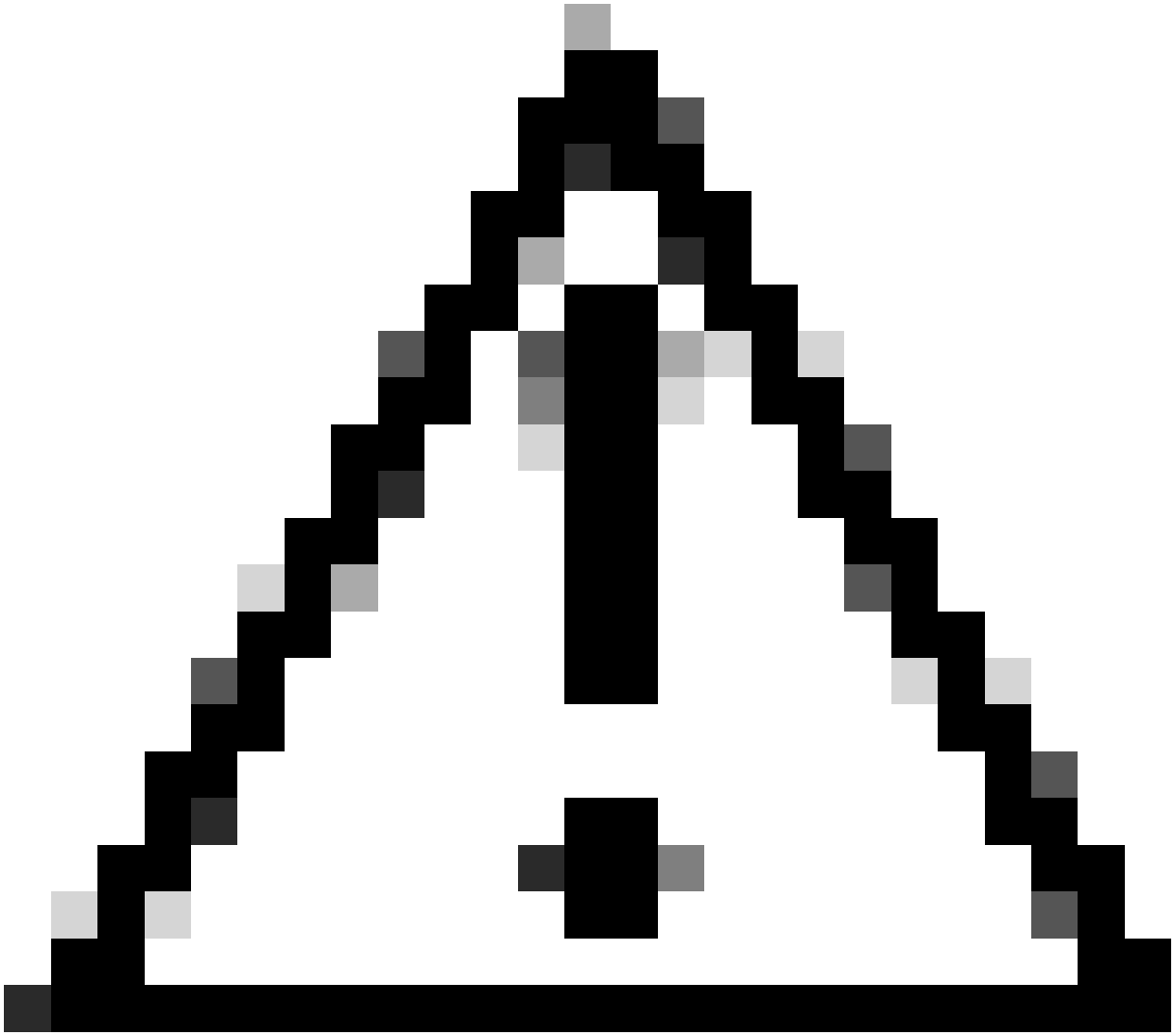
La versión 5 de SOCKS también admite la tunelización UDP, de modo que el cliente también puede utilizar el puerto UDP para enviar el tráfico al proxy. De forma predeterminada, es 16000-16100.

Cuando desea retransmitir un tráfico UDP sobre el proxy SOCKS5, el cliente realiza una solicitud de asociación UDP sobre el puerto de control TCP 1080. El servidor SOCKS5 (SWG/WSA) devuelve un puerto UDP disponible al cliente para enviar paquetes UDP. De forma predeterminada, es 16000-16100. Puede modificar los números de puerto.

A continuación, el cliente comienza a enviar los paquetes UDP que deben retransmitirse al nuevo puerto UDP disponible en el servidor SOCKS5. El servidor SOCKS5 redirige estos paquetes UDP al servidor remoto y redirige los paquetes UDP que provienen del servidor remoto de vuelta al PC.

Cuando desee finalizar la conexión, el PC envía un paquete FIN a través de TCP. El servidor SOCKS5 finaliza la conexión UDP creada para el cliente y, a continuación, finaliza la conexión

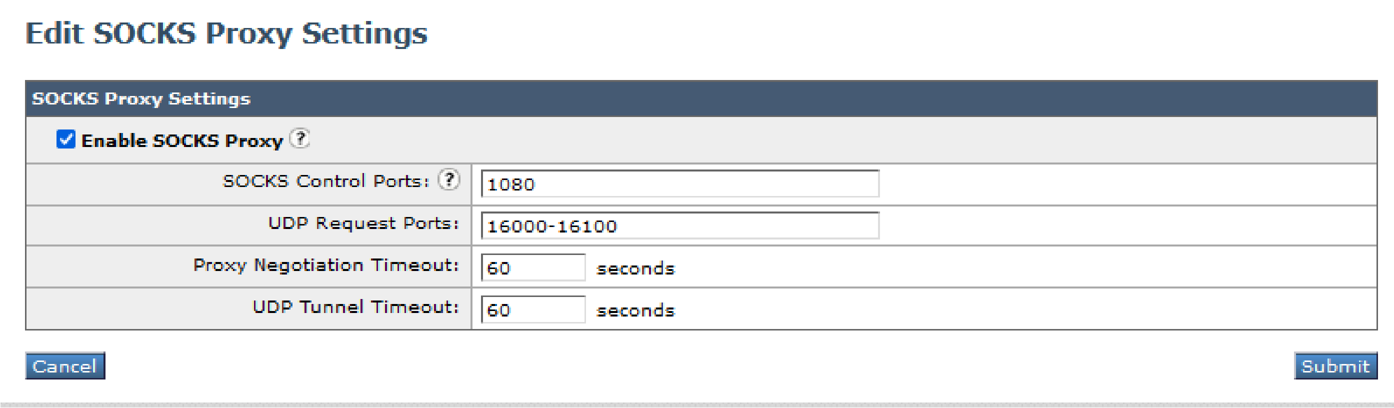
TCP.



Precaución: la información de este documento se creó a partir de los dispositivos de un entorno de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

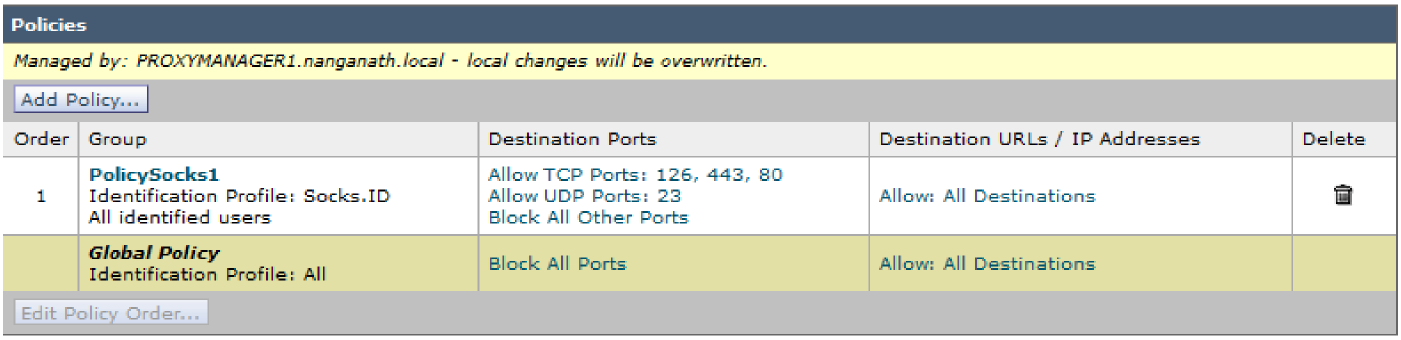
Configuración de proxy SOCKS en SWA/WSA

Puede navegar hasta Servicios de seguridad > Proxy SOCKS para configurar el puerto de control SOCKS y los puertos de solicitud UDP. Esto también permite configurar los tiempos de espera.



Las políticas SOCKS se pueden configurar navegando hasta Administrador de seguridad web > Proxy SOCKS.

Puede configurar las directivas según sea necesario y permitir puertos TCP/UDP específicos según sea necesario



Order	Group	Destination Ports	Destination URLs / IP Addresses	Delete
1	PolicySocks1 Identification Profile: Socks.ID All identified users	Allow TCP Ports: 126, 443, 80 Allow UDP Ports: 23 Block All Other Ports	Allow: All Destinations	
	Global Policy Identification Profile: All	Block All Ports	Allow: All Destinations	

Solucionar problemas relacionados con el proxy SOCKS

Puede ver los registros mediante el seguimiento web en la sección SOCKS del módulo de informes WSA o a través de los registros de acceso.

1652931442.472 0 10.106.37.183 SOCKS_TCP_MISS/200 0 SOCKS_HELLO/ - NONE/- - ALLOW_ADMIN_SOCKS_ALL_CONNECTIONS_11-PolicySocks1-Socks.ID-NONE-NONE-NONE-NONE <"-",-,"-",-,-,-,-,-,-"-,-,-"-,- -,"-","-",-,-"-,-",-"-",-",-",-",-",-"-",-"-",-",-",-",-",-,-",-",-,-"-,"-",-",-,-> - [Detalles de la solicitud: ID = 2428020, Agente de usuario = -, Afiliación al grupo AD = (NINGUNO) -] ; "19/mayo/2022:0 9:07:22 +0530"

1652931442.488 16 10.106.37.183 SOCKS_TCP_MISS/200 338 SOCKS_CONNECT tunnel://151.101.130.219:80/ - DIRECT/151.101.130.219 - ALLOW_ADMIN_SOCKS_ALL_CONNECTIONS_11-PolicySocks1-Socks.ID-NONE-NONE-NONE-NONE-NONE-,-, ","-",-,-,-,-,"-",-,-,-,"-,-,-,"-",-",-,-,-",-,-",-",-",-",-",-",-",-",-",169.00,0,-,"-","-",-,-"-,-"-,-,-",-,-,-"-,-,-"-,-> - [ID = 2428030, Agente = -, Pertenencia a grupos AD = (NONE) -]; "19/May/2022:09:07:22 +0530", IP de servidor = 151.101.130.219

No compatible con la implementación de SWA SOCKS

1. SOCKS versión 5 es compatible. La versión 4 no es compatible.
2. El protocolo SOCKS sólo admite conexiones directas de reenvío, por lo que no admite redirecciones.
3. El proxy SOCKS no admite proxies upstream, por lo que no puede enviar el tráfico socks de WSA a otro proxy upstream. Siempre debe utilizar la directiva de enrutamiento de conexión directa.
4. No puede utilizar las funcionalidades de WSA, como escaneo, AVC, DLP y detección de malware.
5. El rastreo de políticas no puede funcionar con el proxy socks.
6. No hay soporte de descifrado SSL disponible como los túneles de tráfico de cliente a servidor.
7. El proxy Socks sólo admite autenticación básica.

Additional Information

De forma predeterminada, cuando se intenta enviar tráfico SOCKS a través de Firefox, la resolución DNS se realiza de forma local, por lo que WSA no ve ningún nombre de host en los informes ni en los registros de acceso. Si habilitamos el DNS remoto en Firefox, WSA puede resolver el DNS y podemos ver el nombre de host en los registros de informes y acceso. La opción DNS remoto está disponible en las últimas versiones de Firefox. Si no está disponible, siga estos pasos.

acerca de:config
Nombre de preferencia de búsqueda: proxy, busque network.proxy.socks_remote_dns y establézcalo en True.

De forma predeterminada, el navegador Google Chrome realiza la resolución de DNS en el proxy SOCKS, por lo que no es necesario realizar ningún cambio.

Según el documento de soporte de Google Chrome Proxy, SOCKSv5 solo se utiliza para proxy solicitudes de URL basadas en TCP. No se puede utilizar para retransmitir tráfico UDP.

Referencia

https://www.rfc-editor.org/rfc/rfc1928#section-4

https://chromium.googlesource.com/chromium/src/+/HEAD/net/docs/proxy.md#SOCKSv5-proxy-scheme

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).