Configuration et examen du proxy SOCKS sur l'appareil Web sécurisé

Table des matières

Introduction

Ce document décrit comment le proxy SOCKS fonctionne sur Cisco SWA et fournit une vue d'ensemble de la façon dont il achemine le trafic entre un client et le serveur final

Fonctionnement du proxy SOCKS à un niveau élevé

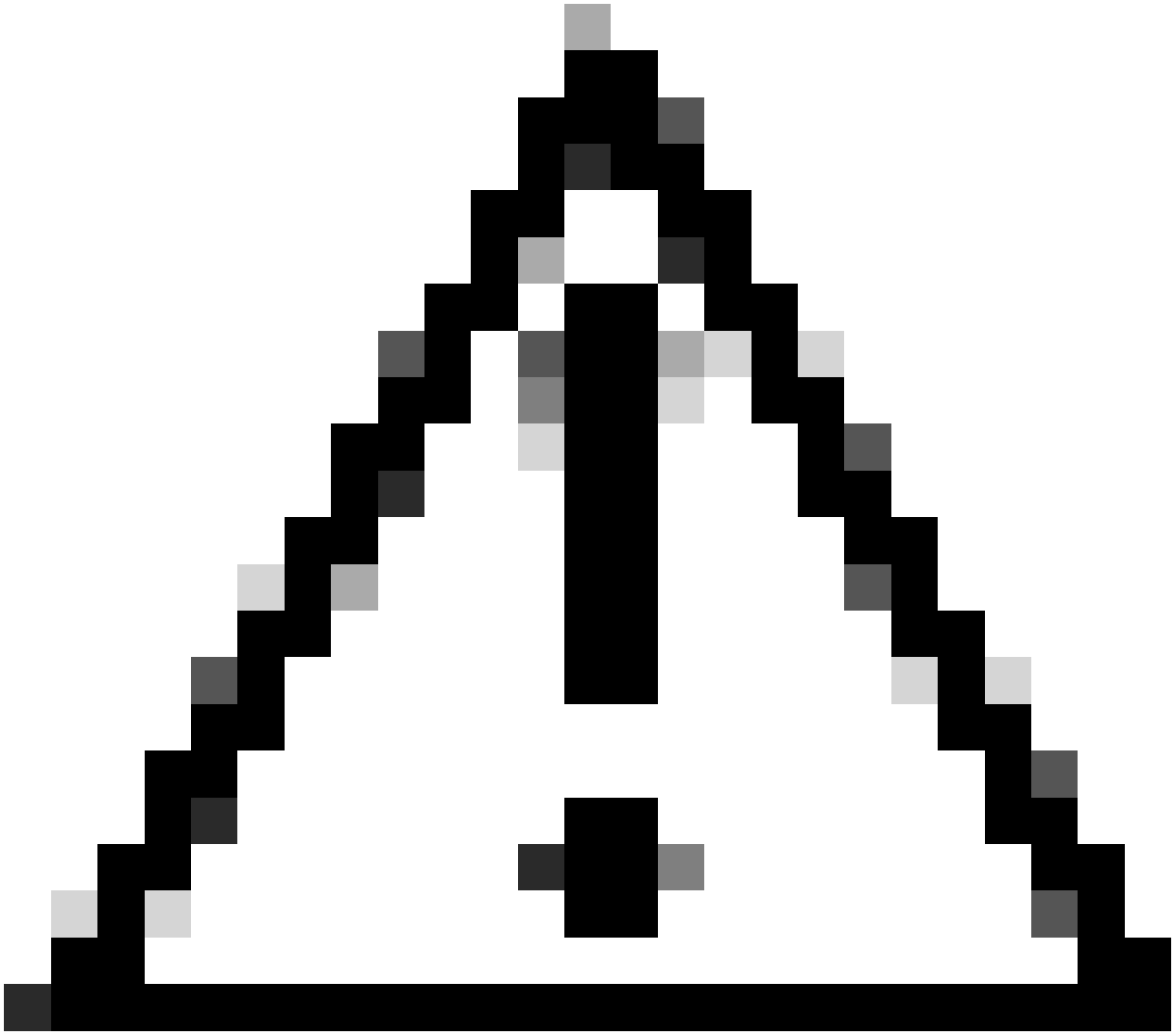
Socket Secure (SOCKS) est un protocole réseau qui facilite la communication avec les serveurs via un proxy SOCKS (ici, il s'agit de SWA/WSA) en acheminant le trafic réseau vers le serveur réel pour le compte d'un client. SOCKS est conçu pour acheminer tout type de trafic de couche application généré par un programme quelconque.
Le SWA utilise par défaut le port TCP 1080 pour écouter le trafic SOCKS du client. Les clients peuvent configurer pour envoyer le trafic socks à WSA sur le port TCP 1080. Vous pouvez ajouter des numéros de port supplémentaires si nécessaire.

SOCKS version 5 prend également en charge la tunnellisation UDP afin que le client puisse également utiliser le port UDP pour envoyer le trafic au proxy. Par défaut, il est 16000-16100.

Lorsque vous souhaitez relayer un trafic UDP sur le proxy SOCKS5, le client effectue une requête d'association UDP sur le port de contrôle TCP 1080. Le serveur SOCKS5 (SWG/WSA) renvoie ensuite un port UDP disponible au client pour l'envoi des packages UDP. Par défaut, il est 16000-16100. Vous pouvez modifier les numéros de port.

Le client commence alors à envoyer les paquets UDP qui doivent être relayés vers le nouveau port UDP disponible sur le serveur SOCKS5. Le serveur SOCKS5 redirige ces packages UDP vers le serveur distant et redirige les packages UDP provenant du serveur distant vers le PC.

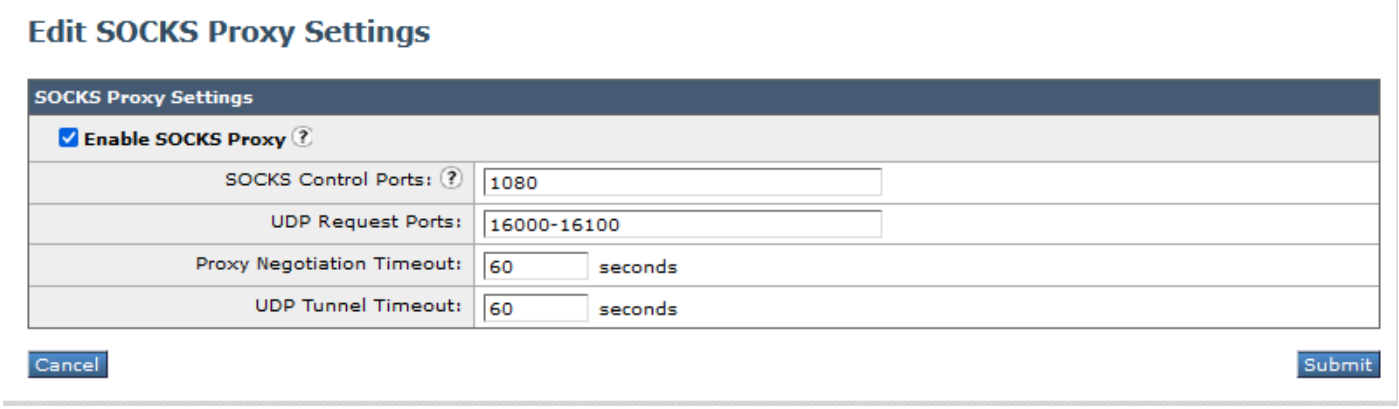
Lorsque vous souhaitez mettre fin à la connexion, le PC envoie un package FIN sur le TCP. Le serveur SOCKS5 met fin à la connexion UDP créée pour le client, puis à la connexion TCP.



Attention : les informations de ce document ont été créées à partir des périphériques d'un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

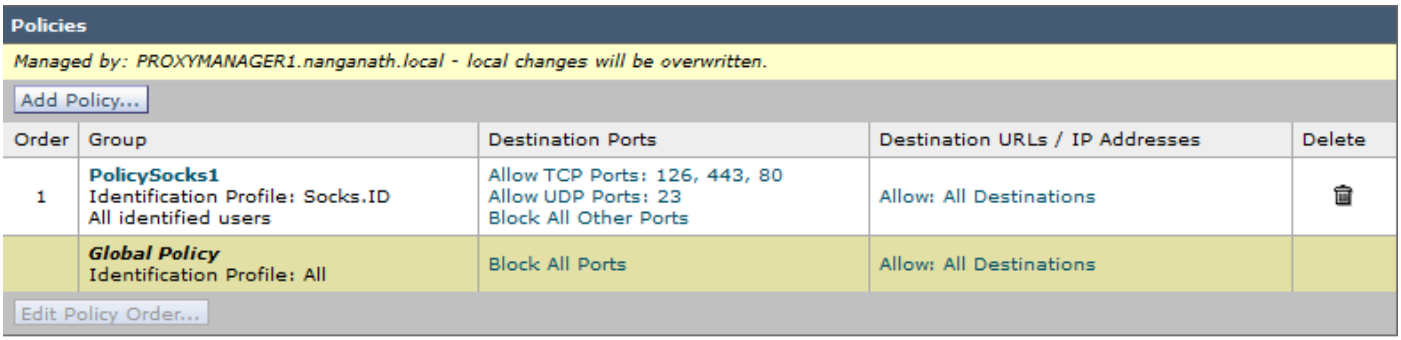
Configuration du proxy SOCKS sur SWA/WSA

Vous pouvez naviguer jusqu'à Services de sécurité > Proxy SOCKS pour configurer le port de contrôle SOCKS et les ports de requête UDP. Cela permet également de configurer les délais d'attente.



Vous pouvez configurer les stratégies SOCKS en accédant à Gestionnaire de sécurité Web > Proxy SOCKS.

Vous pouvez configurer les stratégies selon vos besoins et autoriser des ports TCP/UDP spécifiques selon vos besoins



Résoudre les problèmes liés au proxy SOCKS

Vous pouvez afficher les journaux via le suivi Web dans la section SOCKS du module de rapport WSA ou via les journaux d'accès.

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-NONE-NONE <"-",-,-,-"-,-,-,-,-"-","-"- ,-,-,"-",-,"-","-","-",-,"-",-,"-",-,"-","-","-",-,"-",-,0.00,0,-,"-",-,"-",-,-,-"-,-"-,-",-,-"-,-,-> - - [Détails de la demande : ID = 2428020, Agent utilisateur = -, Appartenances au groupe AD = (AUCUNE) -] ; "19/May/2022:09:07:22 +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 <"-"-,-,"-",- ,-,-,"-",-,-,-,"-,-,-,-,"-","-",-,-,-,"-",-,"-",-,"-",-,"-",-,"-",-,"-",-,"-",-,"-",-,"-",-,169.00,0,-,-",-,"-",-,-"-,-,-"-,-",-,"-",-,-,-,"-,-",-,-> - [Détails de la demande : ID = 2428030, Agent utilisateur = -, Appartenances au groupe AD = ("NONE) - 19/May/2022:09:07:22 +0530", IP du serveur = 151.101.130.219

Non pris en charge dans la mise en oeuvre SWA SOCKS

1. SOCKS version 5 est pris en charge. Version 4 non prise en charge.
2. Le protocole SOCKS ne prend en charge que les connexions directes et ne peut donc pas prendre en charge les redirections.
3. Le proxy SOCKS ne prend pas en charge les proxys en amont, de sorte que vous ne pouvez pas envoyer le trafic SOCKS WSA à un autre proxy en amont. Vous devez toujours utiliser la stratégie de routage de connexion directe.
4. Vous ne pouvez pas utiliser les fonctionnalités WSA telles que l'analyse, AVC, DLP et la détection de programmes malveillants.
5. La trace de stratégie ne peut pas fonctionner avec le proxy socks.
6. Aucune prise en charge du déchiffrement SSL n'est disponible car le trafic passe d'un client à un serveur.
7. Le proxy Socks prend uniquement en charge l'authentification de base.

Additional Information

Par défaut, lorsque vous tentez d'envoyer du trafic SOCKS via Firefox, la résolution DNS est effectuée localement, par conséquent le WSA ne voit aucun nom d'hôte dans les rapports ou les journaux d'accès. Si nous activons le DNS distant sur Firefox, WSA peut effectuer la résolution DNS et nous pouvons afficher le nom d'hôte dans les journaux de rapports/d'accès. L'option DNS distant est disponible dans les dernières versions de Firefox. Si ce n'est pas le cas, procédez comme suit.

à propos:config
Nom de la préférence de recherche : proxy, recherchez network.proxy.socks_remote_dns et définissez-le sur True.

Par défaut, le navigateur Google Chrome effectue la résolution DNS sur le proxy SOCKS. Aucune modification n'est donc nécessaire.

Selon le document de support Google chrome Proxy, SOCKSv5 est uniquement utilisé pour proxy des requêtes d'URL basées sur TCP. Il ne peut pas être utilisé pour relayer le trafic UDP.

Référence

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

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.