在安全Web裝置上配置並檢查SOCKS代理

目錄

簡介

本文檔介紹SOCKS代理如何在Cisco SWA上工作，並概述它如何在客戶端和終端伺服器之間路由流量

SOCKS代理在高級別的工作方式

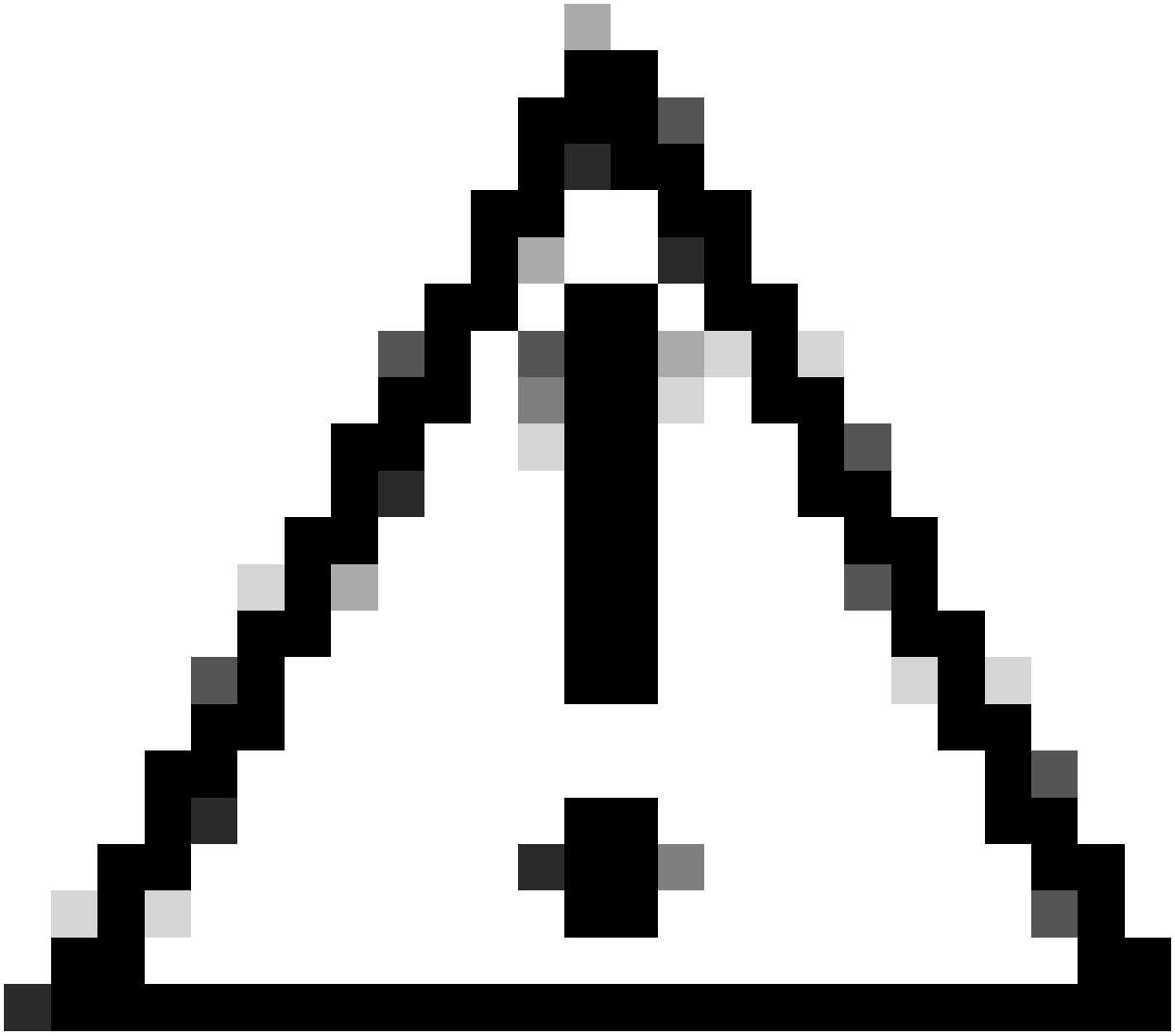
Socket Secure (SOCKS)是一種網路通訊協定，可代表使用者端將網路流量路由至實際伺服器，藉此透過SOCKS代理（此處為SWA/WSA）促進與伺服器的通訊。SOCKS旨在路由任何程式生成的任何型別的應用層流量。
SWA預設使用TCP埠1080監聽客戶端SOCKS流量。客戶端可以配置為將socks流量傳送到TCP埠1080上的WSA。如果需要，可以增加其他埠號。

SOCKS版本5也支援UDP通道，因此使用者端可以使用UDP連線埠將流量傳送至Proxy。依預設，其值為16000-16100。

當您想要透過SOCKS5代理中繼UDP流量時，客戶端會透過TCP控制埠1080發出UDP關聯請求。SOCKS5伺服器(SWG/WSA)接著會傳回可用的UDP連線埠給使用者端，以傳送UDP封裝到。依預設，其值為16000-16100。您可以修改埠號。

然後，客戶端開始傳送需要中繼到SOCKS5伺服器上可用的新UDP埠的UDP包。SOCKS5伺服器將這些UDP包重定向到遠端伺服器，並將來自遠端伺服器的UDP包重定向回電腦。

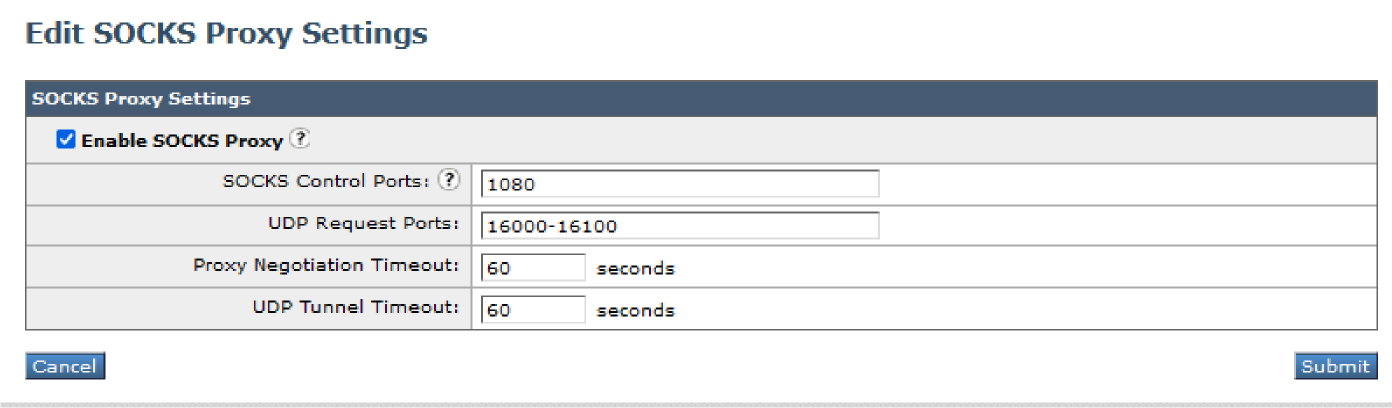
當您想要終止連線時，PC會透過TCP傳送FIN資料包。然後SOCKS5伺服器終止為客戶端建立的UDP連線，然後終止TCP連線。



注意：本文檔中的資訊是根據特定實驗室環境中的裝置建立的。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

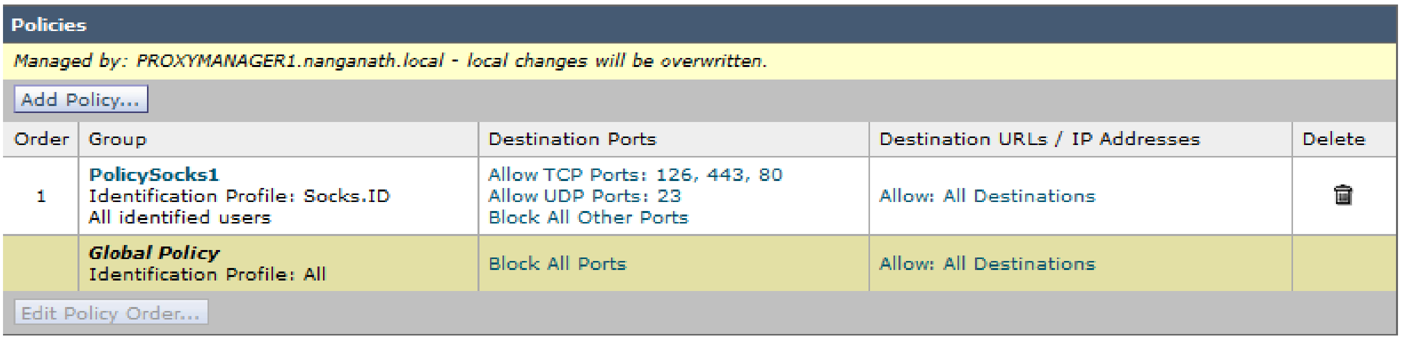
SWA/WSA上的SOCKS代理配置

您可以導航到安全服務> SOCKS代理來配置SOCKS控制埠和UDP請求埠。這也允許配置超時。



可以導航到網路安全管理器> SOCKS代理配置SOCKS策略。

您可以根據需要配置策略，也可以根據需要允許特定TCP/UDP埠



對SOCKS代理相關問題進行故障排除

您可以透過WSA報告模組SOCKS部分的Web跟蹤或透過訪問日誌檢視日誌。

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 <"-"-"、-、"-、"-、"-、-、- 、"- , - , "-"-" , "-"-" , "-"-"-"-"-"-"-" , 0.00,0 , -"-"-"-"-"-"-"-"-"-"-"-"-"-"- , -"-"- , -"-"-"-"-"-"-"-"-"- , -> - [Request Details： ID = 2428020， User Agent = - ， AD Group Membership = (NONE) -] ； 「2022年5月19日：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<"-"-"-"-"-"-"-"-"-"-"-"-"-"-"-"-"-"- 、-、-、"-"、-、-、"-"、-、-、"-"、"-"-"、-、-、"-"、"-"、"-"、"-"、"-"、"-"、"-"、169.00、 0 , - , "-"-"-"- , "-"-"- , -"-"-"-"-"- , - , "-"-"- , - , -> - - - [請求詳細資訊：ID = 2428030，使用者代理= - ， AD組成員資格= (NONE) -] ； 「2022年5月19日：09:07:22 +0530」，伺服器IP = 151.101.130.219

在SWA SOCKS實作中不支援

1. 支援SOCKS版本5。不支援版本4。
2. SOCKS協定僅支援直接轉發連線，因此不能支援重定向。
3. SOCKS代理不支援上游代理，因此您無法將WSA socks流量傳送到另一個上游代理。您必須始終使用直接連線路由策略。
4. 您無法使用WSA功能，例如掃描、AVC、DLP和惡意軟體檢測。
5. 策略跟蹤無法與socks代理一起使用。
6. 從客戶端到伺服器的流量隧道不支援SSL解密。
7. Socks代理僅支援基本身份驗證。

其他資訊

預設情況下，嘗試透過Firefox傳送SOCKS流量時，DNS解析在本地進行，因此WSA在報告或訪問日誌中看不到任何主機名。如果在Firefox上啟用遠端DNS，則WSA可以執行DNS解析，並且可以在報告/訪問日誌中檢視主機名。Remote DNS選項在最新的Firefox版本中可用。如果不可用，請嘗試以下步驟。

關於：config
搜尋首選項名稱：proxy，查詢network.proxy.socks_remote_dns並將其設定為True。

預設情況下，Google Chrome瀏覽器在SOCKS代理上執行DNS解析，因此不需要更改。

根據Google Chrome Proxy支援檔案，SOCKSv5僅用於代理基於TCP的URL要求。它不能用於中繼UDP流量。

參考

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

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。