# セキュアWebアプライアンスでのSOCKSプロキシの設定と確認

## 内容



## はじめに

このドキュメントでは、SOCKSプロキシがCisco SWAでどのように動作するかについて説明し、クライアントとエンドサーバ間のトラフィックをルーティングする方法の概要を示します

## SOCKSプロキシの動作の仕組み

Socket Secure(SOCKS)は、クライアントに代わってネットワークトラフィックを実際のサーバにルーティングすることにより、SOCKSプロキシ（ここではSWA/WSA）を介したサーバとの通信を容易にするネットワークプロトコルです。SOCKSは、任意のプログラムによって生成された任意のタイプのアプリケーション層トラフィックをルーティングするように設計されています。デフォルトでは、SWAはTCPポート1080を使用してクライアントSOCKSトラフィックをリッスンします。クライアントは、TCPポート1080でWSAにSOCKSトラフィックを送信するように設定できます。必要に応じて、ポート番号を追加できます。

SOCKSバージョン5はUDPトンネリングもサポートしているため、クライアントはUDPポートを使用してトラフィックをプロキシに送信することもできます。デフォルトでは、16000-16100です。

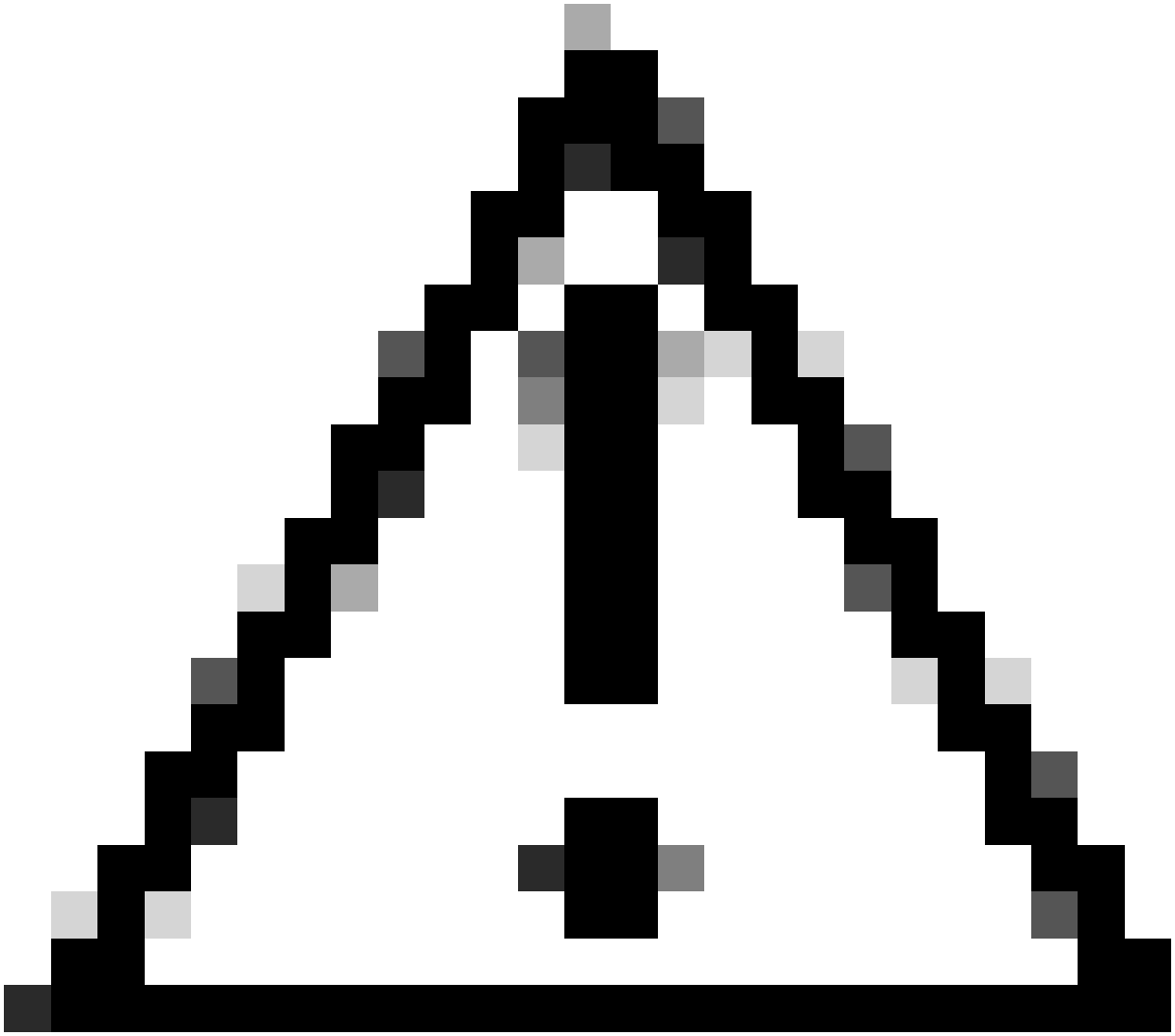
SOCKS5プロキシを介してUDPトラフィックをリレーする場合、クライアントはTCP制御ポート1080を介してUDPアソシエーション要求を行います。SOCKS5サーバ(SWG/WSA)は、UDPパッケージを送信するクライアントに使用可能なUDPポートを返します。デフォルトでは、16000-16100です。ポート番号は変更できます。

次に、クライアントはSOCKS5サーバで利用可能な新しいUDPポートにリレーする必要があるUDPパッケージの送信を開始します。SOCKS5サーバは、これらのUDPパッケージをリモートサーバにリダイレクトし、リモートサーバから送られてきたUDPパッケージをPCにリダイレクトします。

接続を終了する場合、PCはTCP経由でFINパッケージを送信します。次に、SOCKS5サーバは、

クライアント用に作成されたUDP接続を終了し、TCP接続を終了します。

---

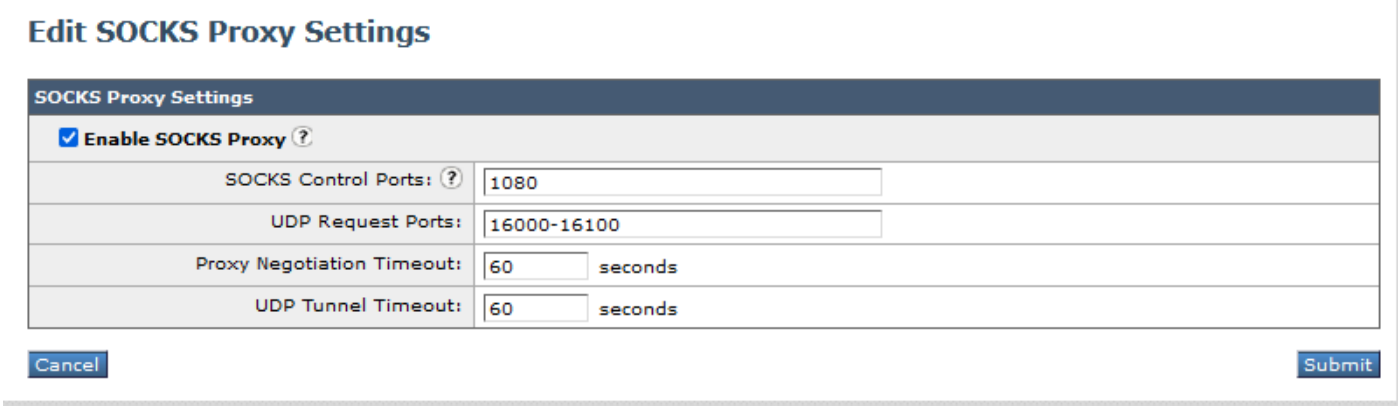


注意：このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

---

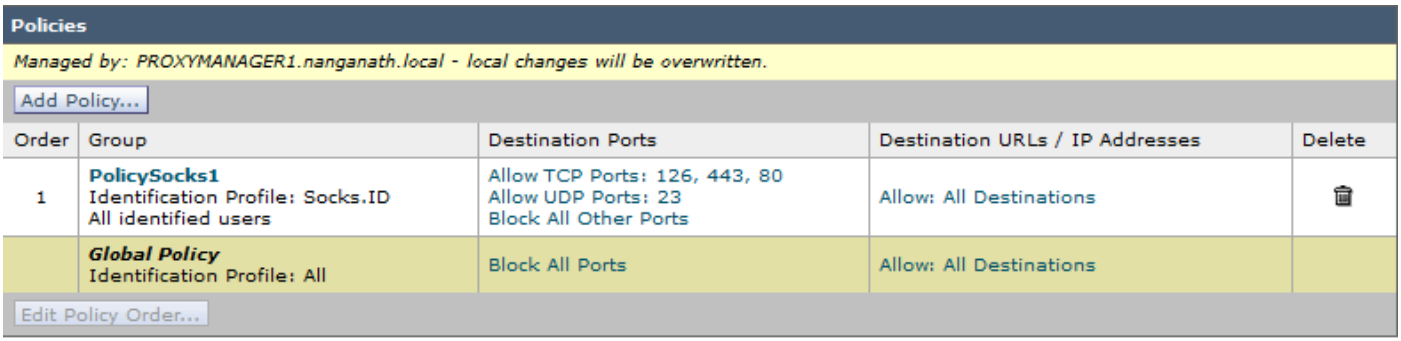
## SWA/WSA上のSOCKSプロキシ設定

Security services > SOCKS proxyの順に移動して、SOCKS制御ポートとUDP要求ポートを設定できます。これにより、タイムアウトを設定することもできます。




SOCKSポリシーは、Web Security Manager > SOCKS Proxyに移動して設定できます。

必要に応じてポリシーを設定したり、特定のTCP/UDPポートを許可したりできます




# SOCKSプロキシ関連の問題のトラブルシューティング

ログは、WSAレポートモジュールのSOCKSセクションのWebトラッキングまたはアクセスログを通じて表示できます。

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 Memberships = ( 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-PolcySocks1-Socks.ID-NONE-NONE-NONE<"- 、-、"-"、-、-、-、-、"-"、-、-、"-、-、"-、"-、"-、"-、"-、"-、"-、"-、"-、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、"-"、",169 .00,0,-,"-","-","-,"-","-","-,"-","-","-","-","-,-,"-","-,"-,-> - [要求の詳細： ID = 2428030, User Agent = -, AD Group Memberships = ( NONE ) - ]; 「2022年5月19日：09:07:22 +0530」、サーバIP = 151.101.130.219

# SWA SOCKS実装ではサポートされない

1. SOCKSバージョン5がサポートされます。バージョン4はサポートされていません。
2. SOCKSプロトコルは直接転送接続のみをサポートするため、リダイレクトはサポートできません。
3. SOCKSプロキシはアップストリームプロキシをサポートしないため、WSA SOCKSトラフィックを別のアップストリームプロキシに送信することはできません。直接接続ルーティングポリシーを常に使用する必要があります。
4. スキャン、AVC、DLP、マルウェア検出などのWSA機能は使用できません。
5. ポリシートレースはSOCKSプロキシでは動作しません。
6. クライアントからサーバへのトラフィックトンネルとして使用できるSSL復号化サポートはありません。
7. SOCKSプロキシは基本認証のみをサポートします。

# 追加情報

デフォルトでは、Firefox経由でSOCKSトラフィックを送信しようとすると、DNS解決がローカルに行われます。そのため、WSAはレポートログやアクセスログでホスト名を確認できません。FirefoxでリモートDNSを有効にすると、WSAはDNS解決を実行でき、レポート/アクセスログでホスト名を表示できます。リモートDNSオプションは、最新バージョンのFirefoxで使用できます。使用できない場合は、次の手順を試してください。

項目詳細：設定
Search Preference name : proxyと入力し、network.proxy.socks_remote_dnsを検索してTrueに設定します。

Google Chromeブラウザはデフォルトで SOCKSプロキシのDNS解決を実行するため、変更は必要ありません。

Google chromeプロキシサポートドキュメントによると、SOCKSv5はTCPベースのURL要求のプロキシにのみ使用されます。UDPトラフィックのリレーには使用できません。

# 参考

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

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。