在安全网络设备上配置并检查SOCKS代理

目录

简介

本文档介绍SOCKS代理如何在Cisco SWA上工作，并概述它如何在客户端和终端服务器之间路由流量

SOCKS代理在高级别的工作方式

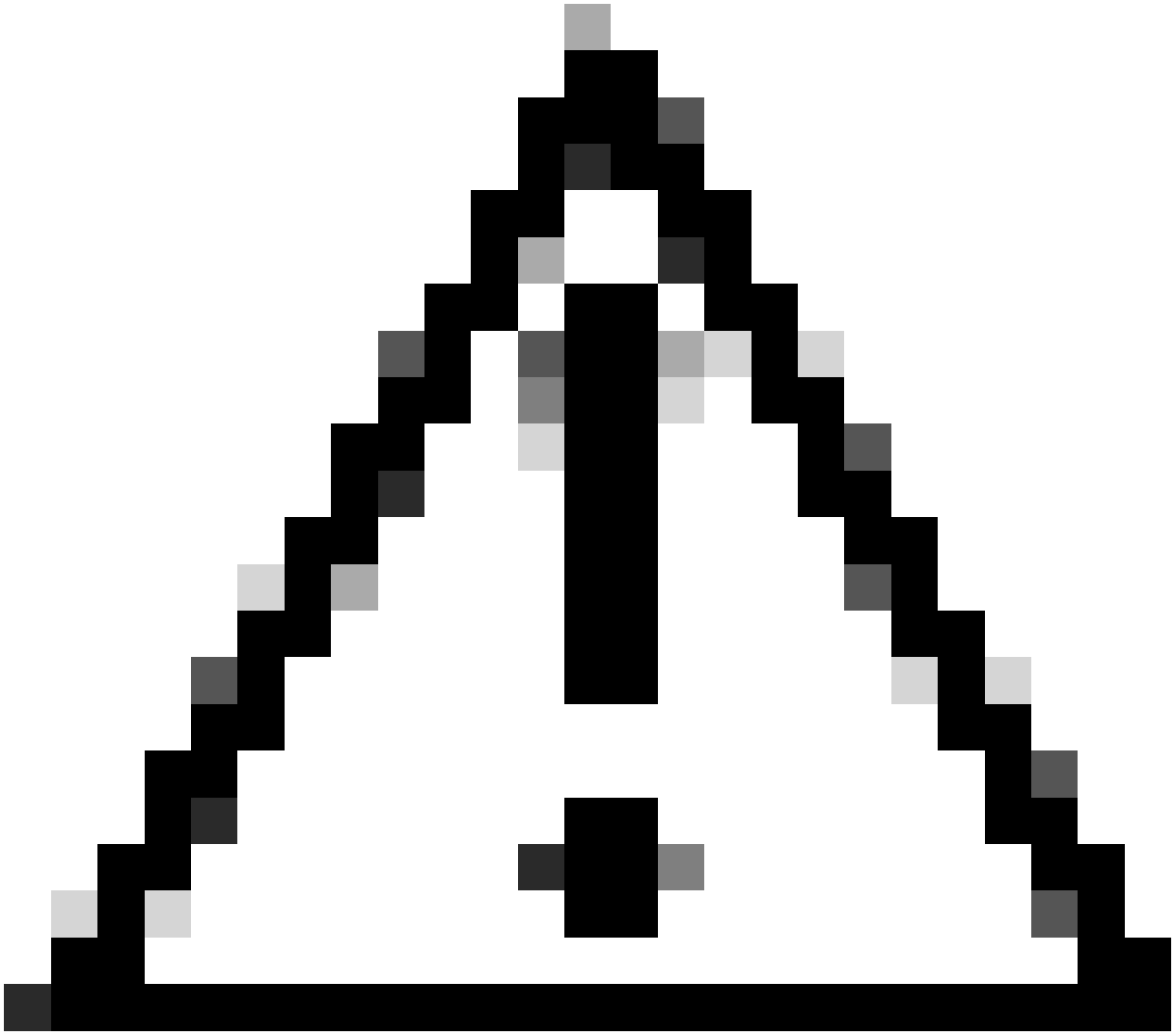
Socket Secure (SOCKS)是一种网络协议，它通过代表客户端将网络流量路由到实际服务器，促进通过SOCKS代理（此处为SWA/WSA）与服务器的通信。SOCKS用于路由任何程序生成的任何类型的应用层流量。
SWA默认使用TCP端口1080监听客户端SOCKS流量。客户端可以配置为将socks流量发送到TCP端口1080上的WSA。如果需要，您可以添加其他端口号。

SOCKS版本5还支持UDP隧道，因此客户端也可以使用UDP端口将流量发送到代理。默认情况下，该值为16000-16100。

当您希望通过SOCKS5代理中继UDP流量时，客户端会通过TCP控制端口1080发出UDP关联请求。然后，SOCKS5服务器(SWG/WSA)将可用UDP端口返回到客户端以发送UDP数据包。默认情况下，该值为16000-16100。您可以修改端口号。

然后，客户端开始发送需要中继到SOCKS5服务器上可用的新UDP端口的UDP数据包。SOCKS5服务器将这些UDP包重定向到远程服务器，并将来自远程服务器的UDP包重定向回PC。

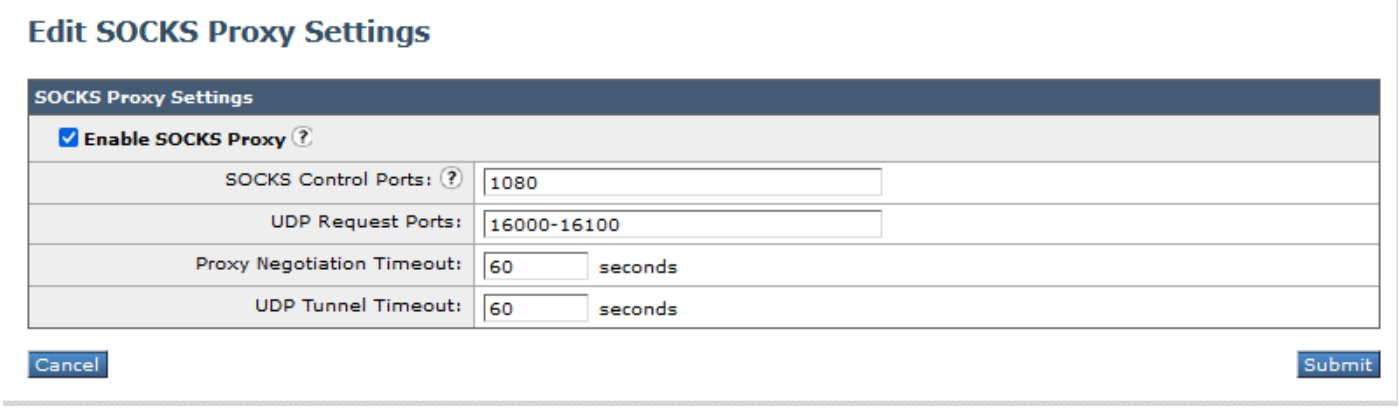
当您想要终止连接时，PC会通过TCP发送FIN数据包。然后，SOCKS5服务器终止为客户端创建的UDP连接，然后终止TCP连接。



注意：本文档中的信息是根据特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

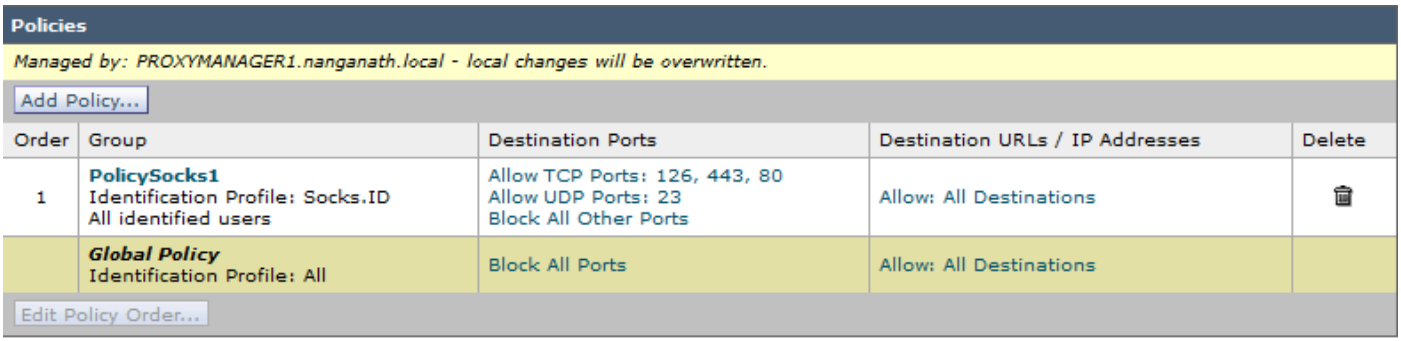
SWA/WSA上的SOCKS代理配置

可以导航到安全服务> SOCKS代理配置SOCKS控制端口和UDP请求端口。这也允许配置超时。



通过导航到网络安全管理器> SOCKS代理可以配置SOCKS策略。

您可以根据需要配置策略，也可以根据需要允许特定TCP/UDP端口



解决SOCKS代理相关问题

您可以通过WSA报告模块SOCKS部分的网络跟踪或访问日志查看日志。

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 <"-"-"、-"-"-、-"-"-"-"-"-"-"-"-" , "-"- , - , "-"-"-"-"-"-" , "-"-"-"-"-" , 0.00,0 , -"-"-"-"-"-"-"-"-"-"-"-"-"-"-"-"- , -"-"-"-"-"-"-"-"-"- , -> - [请求详细信息：ID = 2428020，用户代理= - ，AD组成员= (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 , - , "-" , "-" , "-"-" , - , "-"-"-"-"-"- , -"-"-" , -> - - - [请求详细信息：ID = 2428030，用户代理= - ，AD组成员资格= (NONE) -] ；“2022年5月19日：09:07:22 +0530”，服务器IP = 151.101.130.219

SWA SOCKS实施中不支持

1. 支持SOCKS第5版。不支持版本4。

2. SOCKS协议仅支持直接转发连接，因此它不支持重定向。
3. SOCKS代理不支持上游代理，因此您无法将WSA socks流量发送到另一个上游代理。必须始终使用直接连接路由策略。
4. 您不能使用WSA功能，如扫描、AVC、DLP和恶意软件检测。
5. 策略跟踪无法与socks代理一起使用。
6. 从客户端到服务器的流量隧道不支持SSL解密。
7. Socks代理仅支持基本身份验证。

其他信息

默认情况下，当尝试通过Firefox发送SOCKS流量时，DNS解析在本地进行，因此WSA在报告或访问日志中看不到任何主机名。如果在Firefox上启用远程DNS，则WSA可以执行DNS解析，并且可以在报告/访问日志中查看主机名。Remote DNS选项在最新的Firefox版本中可用。如果不可用，请尝试以下步骤。

关于：配置
搜索首选项名称：proxy，查找network.proxy.socks_remote_dns并将其设置为True。

默认情况下，Google Chrome浏览器在SOCKS代理上执行DNS解析，因此不需要更改。

根据Google Chrome代理支持文档，SOCKSv5仅用于代理基于TCP的URL请求。它不能用于中继UDP流量。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。