Secure Web Appliance에서 SOCKS 프록시 구성 및 검사

목차

소개

이 문서에서는 SOCKS 프록시가 Cisco SWA에서 작동하는 방식을 설명하고 클라이언트와 최종 서버 간에 트래픽을 라우팅하는 방법에 대한 개요를 제공합니다

SOCKS 프록시가 상위 레벨에서 작동하는 방식

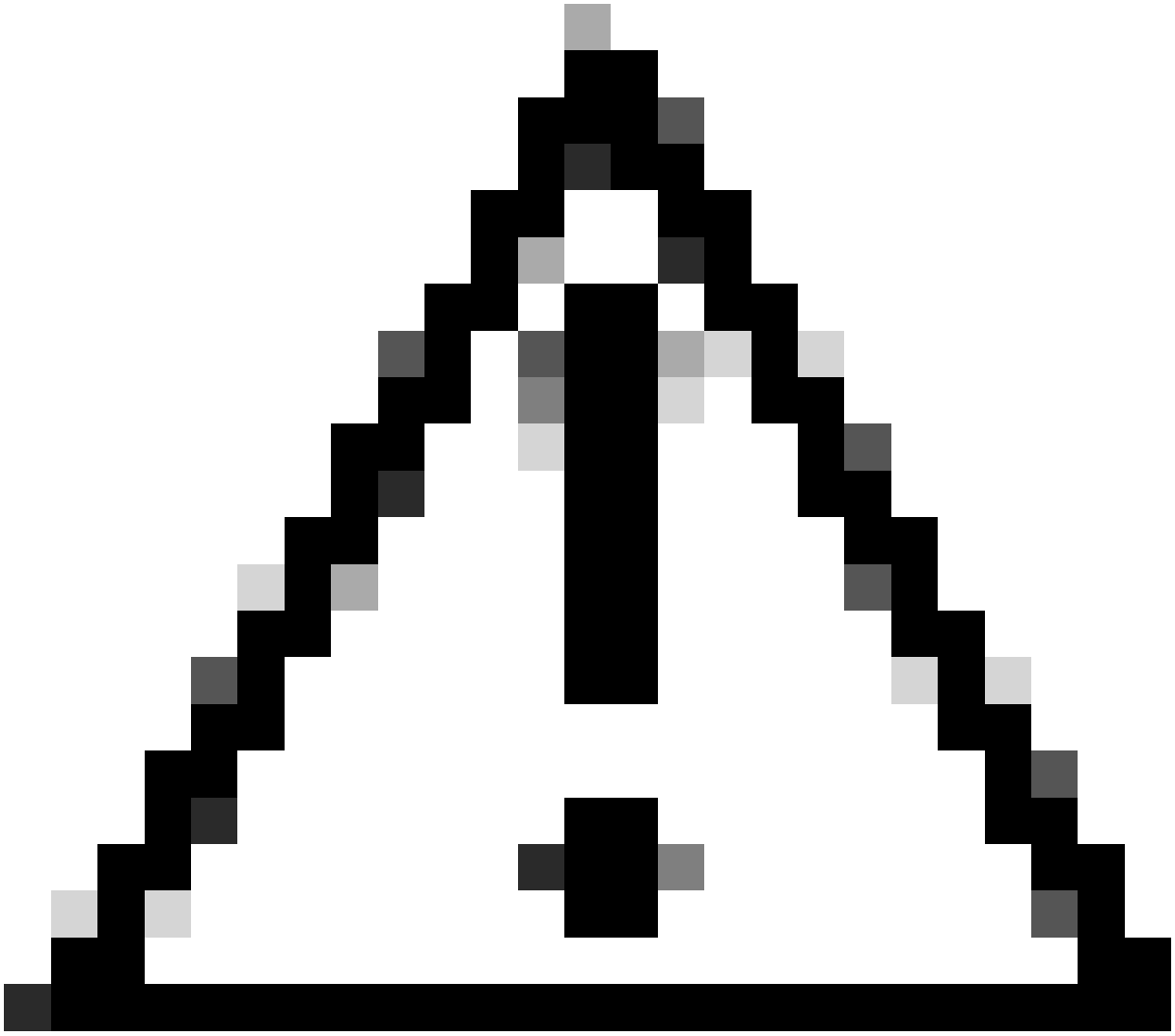
SOCKS(Socket Secure)는 클라이언트를 대신하여 실제 서버에 네트워크 트래픽을 라우팅하여 SOCKS 프록시(여기서는 SWA/WSA)를 통해 서버와의 통신을 용이하게 하는 네트워크 프로토콜입니다. SOCKS는 모든 프로그램에서 생성되는 모든 유형의 애플리케이션 레이어 트래픽을 라우팅하도록 설계되었습니다.
SWA는 기본적으로 TCP 포트 1080을 사용하여 클라이언트 SOCKS 트래픽을 수신합니다. 클라이언트는 TCP 포트 1080에서 WSA로 socks 트래픽을 전송하도록 구성할 수 있습니다. 필요한 경우 추가 포트 번호를 추가할 수 있습니다.

SOCKS 버전 5는 UDP 터널링도 지원하므로 클라이언트가 UDP 포트를 사용하여 트래픽을 프록시로 전송할 수도 있습니다. 기본적으로 16000-16100.

SOCKS5 프록시를 통해 UDP 트래픽을 릴레이하려면 클라이언트는 TCP 제어 포트 1080을 통해 UDP 연결 요청을 합니다. SOCKS5 서버(SWG/WSA)는 사용 가능한 UDP 포트를 클라이언트로 반환하여 UDP 패키지를 전송합니다. 기본적으로 16000-16100. 포트 번호를 수정할 수 있습니다.

그런 다음 클라이언트는 릴레이해야 하는 UDP 패키지를 SOCKS5 서버에서 사용할 수 있는 새 UDP 포트로 보내기 시작합니다. SOCKS5 서버는 이러한 UDP 패키지를 원격 서버로 리디렉션하고 원격 서버에서 오는 UDP 패키지를 다시 PC로 리디렉션합니다.

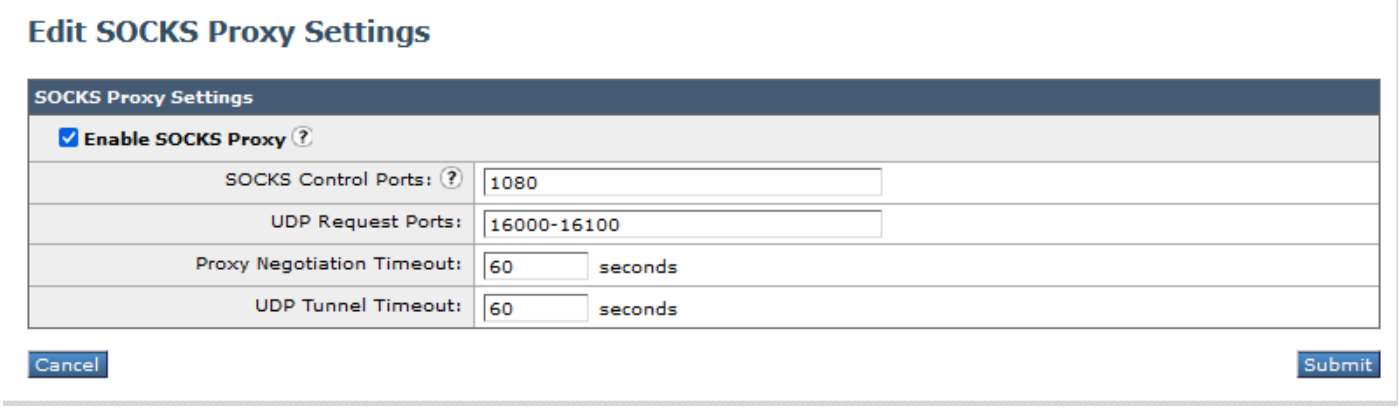
연결을 종료하려는 경우 PC가 TCP를 통해 FIN 패키지를 전송합니다. 그런 다음 SOCKS5 서버는 클라이언트에 대해 생성된 UDP 연결을 종료하고 TCP 연결을 종료합니다.



주의: 이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

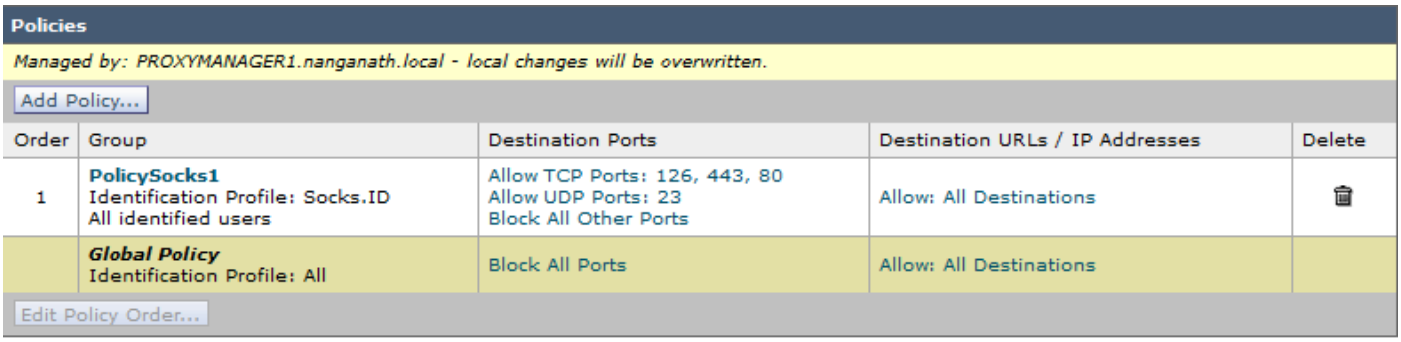
SWA/WSA의 SOCKS 프록시 컨피그레이션

Security services(보안 서비스) > SOCKS proxy(SOCKS 프록시)로 이동하여 SOCKS 제어 포트 및 UDP 요청 포트를 구성할 수 있습니다. 이렇게 하면 시간 초과도 구성할 수 있습니다.



Web Security Manager(웹 보안 관리자) > SOCKS Proxy(SOCKS 프록시)로 이동하여 SOCKS 정책을 구성할 수 있습니다.

필요에 따라 정책을 구성하고 필요에 따라 특정 TCP/UDP 포트를 허용할 수 있습니다



SOCKS 프록시 관련 문제 해결

WSA 보고 모듈 SOCKS 섹션의 웹 추적 또는 액세스 로그를 통해 로그를 볼 수 있습니다.

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,-,"-","-",-,"-",-,-,"-","-",-,"-",-,-> - - [요청 세부 정보: ID = 2428020, 사용자 에이전트 = -, AD 그룹 멤버십 = (없음) -] ; "19/5/2022:09:07:22 +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-NONE <",-,-,-,-,",-,-",-",-",-,-" ,-,"-","-","-","-","-","-","-","-","-","-",",-,"-",-,",-","-",-",-",-",-",-",-,-> - - [요청 정보: ID = 2428030, 사용자 에이전트 = -, AD 그룹 구성원 = (없음) -]; "19/5월 /2022:09:07:22 +0530", 서버 IP = 151.101.130.219

SWA SOCKS 구현에서 지원되지 않음

1. SOCKS 버전 5가 지원됩니다. 버전 4는 지원되지 않습니다.

2. SOCKS 프로토콜은 리디렉션을 지원하지 않도록 직접 전달 연결만 지원합니다.
3. SOCKS 프록시는 업스트림 프록시를 지원하지 않으므로 WSA socks 트래픽을 다른 업스트림 프록시로 전송할 수 없습니다. 항상 직접 연결 라우팅 정책을 사용해야 합니다.
4. 검사, AVC, DLP 및 악성코드 탐지와 같은 WSA 기능을 활용할 수 없습니다.
5. 정책 추적은 socks 프록시에서 작동할 수 없습니다.
6. 클라이언트에서 서버로 이동하는 트래픽 터널로 SSL 암호 해독 지원을 사용할 수 없습니다.
7. Socks 프록시는 기본 인증만 지원합니다.

추가 정보

기본적으로 Firefox를 통해 SOCKS 트래픽을 전송하려고 하면 DNS 확인이 로컬로 이루어지므로 WSA에서 보고 또는 액세스 로그에 호스트 이름이 표시되지 않습니다. Firefox에서 Remote DNS를 활성화하면 WSA에서 DNS 확인을 수행하고 보고/액세스 로그에서 호스트 이름을 볼 수 있습니다. Remote DNS 옵션은 최신 Firefox 버전에서 사용할 수 있습니다. 사용할 수 없는 경우 다음 단계를 수행합니다.

정보:config
검색 기본 설정 이름 : proxy, network.proxy.socks_remote_dns를 찾아 True로 설정합니다.

Google Chrome 브라우저는 기본적으로 SOCKS 프록시에서 DNS 확인을 수행하므로 변경할 필요가 없습니다.

Google chrome 프록시 지원 문서에 따르면 SOCKSv5는 TCP 기반 URL 요청을 프록시하는 데만 사용됩니다. UDP 트래픽을 릴레이하는 데 사용할 수 없습니다.

참조

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

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.