Konfiguration und Überprüfung des SOCKS-Proxys auf einer sicheren Webappliance

Inhalt

Einleitung

Dieses Dokument beschreibt die Funktionsweise des SOCKS-Proxys auf Cisco SWA und bietet einen Überblick über das Routing von Datenverkehr zwischen einem Client und dem Endserver

So funktioniert der SOCKS-Proxy auf hoher Ebene

Socket Secure (SOCKS) ist ein Netzwerkprotokoll, das die Kommunikation mit Servern über einen SOCKS-Proxy (hier SWA/WSA) ermöglicht, indem der Netzwerkverkehr im Auftrag eines Clients an den eigentlichen Server weitergeleitet wird. SOCKS wurde entwickelt, um jede Art von Anwendungsdatenverkehr weiterzuleiten, der von einem beliebigen Programm generiert wird. Der SWA verwendet standardmäßig den TCP-Port 1080, um den SOCKS-Datenverkehr des Clients zu überwachen. Die Clients können so konfigurieren, dass der Socks-Datenverkehr an WSA auf dem TCP-Port 1080 gesendet wird. Bei Bedarf können Sie weitere Portnummern hinzufügen.

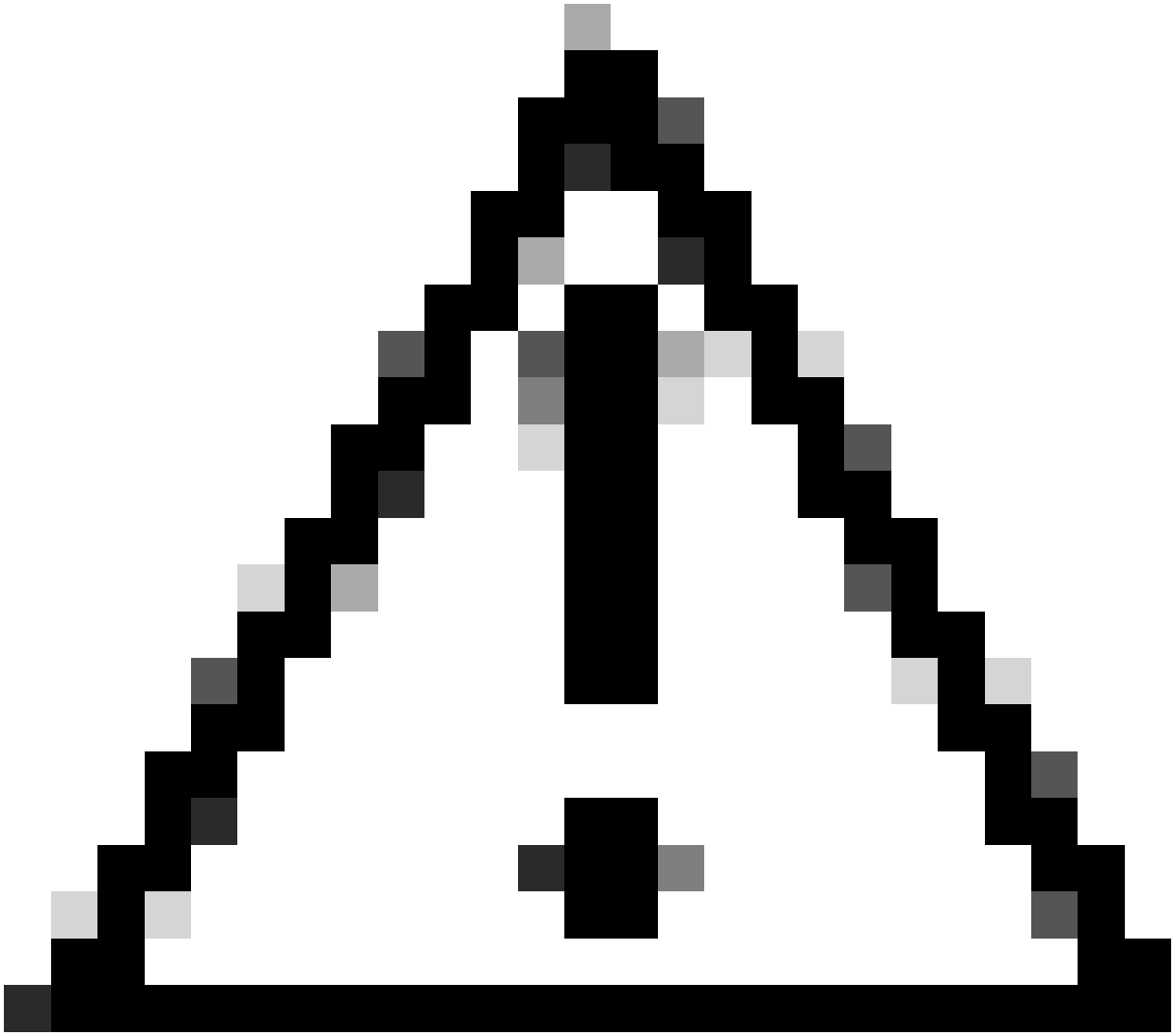
SOCKS Version 5 unterstützt auch UDP-Tunneling, sodass der Client den UDP-Port auch zum Senden des Datenverkehrs an den Proxy verwenden kann. Standardmäßig ist dies 16000-16100.

Wenn Sie einen UDP-Datenverkehr über den SOCKS5-Proxy weiterleiten möchten, sendet der Client eine UDP-Zuordnungsanforderung über den TCP-Steuerungsport 1080. Der SOCKS5-Server (SWG/WSA) gibt dann einen verfügbaren UDP-Port an den Client zurück, an den UDP-Pakete gesendet werden. Standardmäßig ist dies 16000-16100. Sie können die Portnummern ändern.

Der Client sendet dann die UDP-Pakete, die weitergeleitet werden müssen, an den neuen UDP-Port, der auf dem SOCKS5-Server verfügbar ist. Der SOCKS5-Server leitet diese UDP-Pakete zum Remote-Server um und leitet die UDP-Pakete vom Remote-Server zurück zum PC.

Wenn Sie die Verbindung beenden möchten, sendet der PC ein FIN-Paket über das TCP. Der

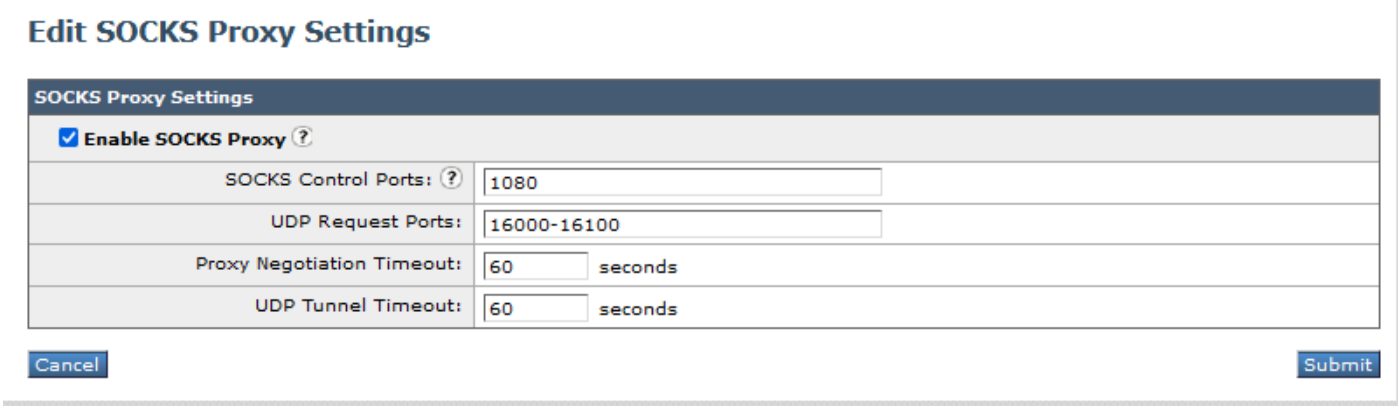
SOCKS5-Server beendet dann die für den Client erstellte UDP-Verbindung und beendet dann die TCP-Verbindung.



Vorsicht: Die Informationen in diesem Dokument stammen von Geräten in einer bestimmten Laborumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

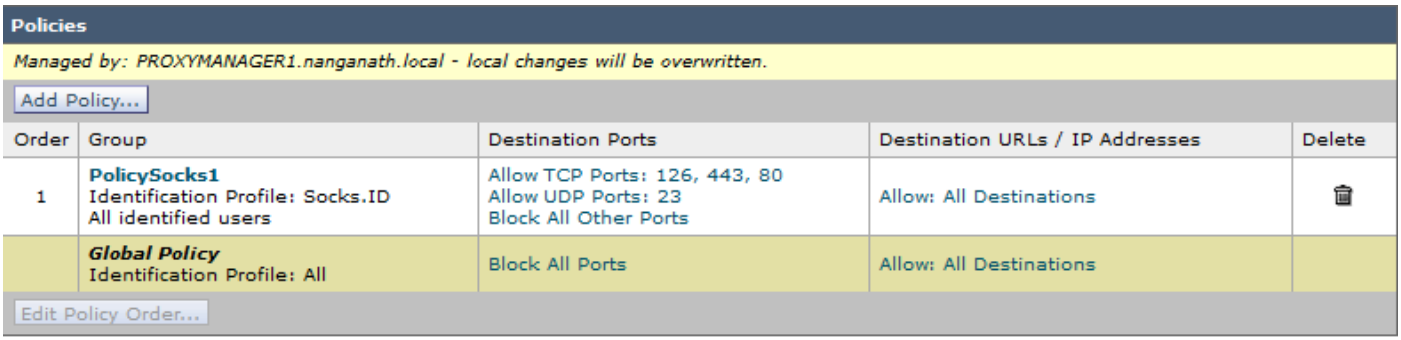
SOCKS-Proxy-Konfiguration auf SWA/WSA

Sie können zu Sicherheitsdienste > SOCKS-Proxy navigieren, um den SOCKS-Steuerungsport und die UDP-Anforderungsports zu konfigurieren. Dies ermöglicht auch die Konfiguration der Timeouts.



SOCKS-Richtlinien können konfiguriert werden, indem Sie zu Websicherheits-Manager > SOCKS-Proxy navigieren.

Sie können die Richtlinien nach Bedarf konfigurieren und bei Bedarf bestimmte TCP-/UDP-Ports zulassen



Fehlerbehebung bei Problemen mit dem SOCKS-Proxy

Sie können die Protokolle im Abschnitt SOCKS des WSA-Reporting-Moduls über Web-Tracking oder über die Zugriffsprotokolle anzeigen.

1652931442.472 0 10.106.37.183 SOCKS_TCP_MISS/200 0 SOCKS_HELLO/ - KEINE/- - ALLOW_ADMIN_SOCKS_ALL_CONNECTIONS_11-PolicySocks1-Socks.ID-NONE-NONE-NONE-NONE-NONE KEINE <"-",-","-",-","-",-,-","-",-","-",-,-","-",-","-",-","-",-","-",-","-",-","-","-","-","-","-","-","-","-","-","-","-","-", 0,00,-, "-","-","-","-",-,-","-",-","-",-,-","-",-,-,-> - - [Anforderungsdetails: ID = 2428020, Benutzeragent = -, AD-Gruppenmitgliedschaften = (KEINE) -] ; "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_CONNECT NECTIONS_11-PolicySocks1-Socks.ID-NONE-NONE-NONE-NONE-NONE <"-",-,-",-",-,-,-,-",-",-,-",-",-",-",-",-",-",-",-",-",-",-", ","-","-","-","-",-",169.00,0,-,"-",-",-,",-",-,-,-",-,-,-",-,-,-> - - [Request Details: ID = 2428030, User Agent = -, AD Group Memberships = (NONE) -]; "1 9/May/2022:09:07:22 +0530", Server-IP = 151.101.130.219

Keine Unterstützung bei SWA SOCKS-Implementierung

1. SOCKS Version 5 wird unterstützt. Version 4 wird nicht unterstützt.
2. Das SOCKS-Protokoll unterstützt nur direkte Weiterleitungsverbindungen, sodass es keine Umleitungen unterstützen kann.
3. Der SOCKS-Proxy unterstützt keine Upstream-Proxys, sodass Sie den WSA-Socks-Datenverkehr nicht an einen anderen Upstream-Proxy senden können. Sie müssen immer die Routingrichtlinie für Direktverbindungen verwenden.
4. Sie können die WSA-Funktionen wie Scanning, AVC, DLP und Malware-Erkennung nicht nutzen.
5. Die Richtlinienverfolgung kann nicht mit dem Socks-Proxy verwendet werden.
6. Es ist keine SSL-Verschlüsselungsunterstützung verfügbar, da der Datenverkehr zwischen Client und Server getunnelt wird.
7. Der Socks-Proxy unterstützt nur die Standardauthentifizierung.

Zusätzliche Informationen

Wenn Sie versuchen, SOCKS-Datenverkehr über Firefox zu senden, wird die DNS-Auflösung standardmäßig lokal vorgenommen, sodass die WSA in den Berichts- oder Zugriffsprotokollen keinen Hostnamen erkennt. Wenn wir Remote DNS auf Firefox aktivieren, kann die WSA die DNS-Auflösung durchführen und den Hostnamen in Berichts-/Zugriffsprotokollen anzeigen. Die Remote DNS-Option ist in den neuesten Firefox-Versionen verfügbar. Wenn es nicht verfügbar ist, probieren Sie diese Schritte aus.

Info:Konfiguration
Suchvoreinstellungsname: proxy, suche network.proxy.socks_remote_dns und setze ihn auf True.

Der Browser Google Chrome führt standardmäßig eine DNS-Auflösung auf dem SOCKS-Proxy aus, sodass keine Änderungen erforderlich sind.

Gemäß dem Google Chrome Proxy-Support-Dokument wird SOCKSv5 nur für TCP-basierte URL-Anfragen verwendet. Er kann nicht für die Weiterleitung von UDP-Datenverkehr verwendet werden.

Referenz

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

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.