

SOCKS Proxy op beveiligde web-applicatie configureren en onderzoeken

Inhoud

[Inleiding](#)

[Hoe SOCKS proxy werkt op een hoog niveau](#)

[SOCKS Proxy-configuratie op SWA/WSA](#)

[Probleemoplossing voor de SOCKS-proxy-gerelateerde problemen](#)

[Niet ondersteund in implementatie SWA SOCKS](#)

[Aanvullende informatie](#)

[Referentie](#)

Inleiding

Dit document beschrijft hoe de SOCKS-proxy aan Cisco SWA werkt en biedt een overzicht van de manier waarop het verkeer tussen een client en de eindserver wordt routeerd

Hoe SOCKS proxy werkt op een hoog niveau

Socket Secure (SOCKS) is een netwerkprotocol dat de communicatie met servers via een SOCKS-proxy (hier is het SWA/WSA) vergemakkelijkt door het netwerkverkeer namens een client naar de feitelijke server te routeren. SOCKS is ontworpen om elk type toepassingslaagverkeer te routeren dat door elk programma wordt gegenereerd.

De SWA maakt standaard gebruik van TCP-poort 1080 om te luisteren naar het client-SOCKS-verkeer. De clients kunnen configureren om het socks-verkeer naar WSA op TCP-poort 1080 te versturen. U kunt indien nodig extra poortnummers toevoegen.

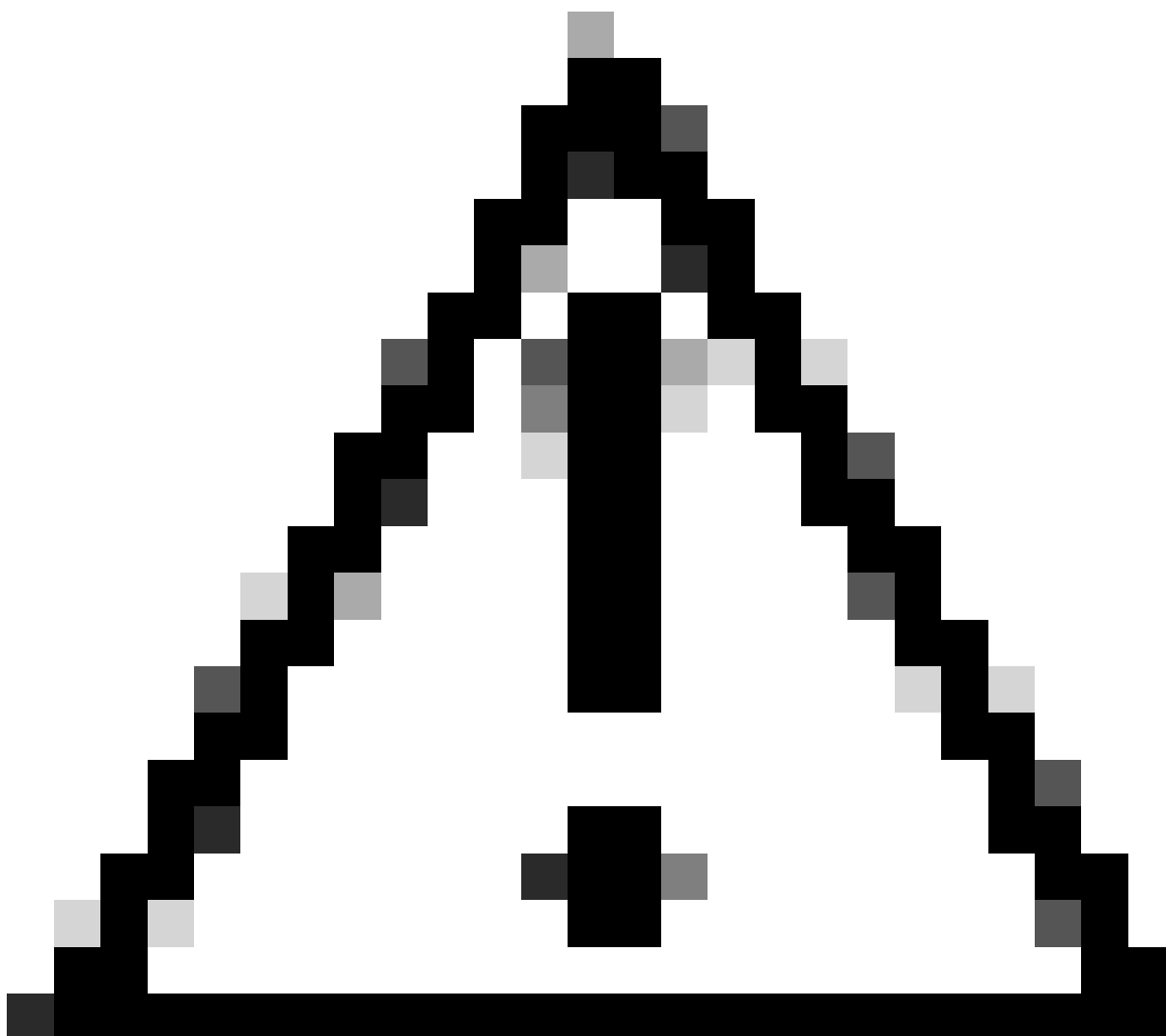
SOCKS versie 5 ondersteunt ook UDP-tunneling, zodat de client ook de UDP-poort kan gebruiken om het verkeer naar de proxy te sturen. Standaard is het 16000-16100.

Wanneer u een UDP-verkeer via de SOCKS5-proxy wilt doorgeven, dient de client een UDP-associatieverzoek in via de TCP-controlepoort 1080. SOCKS5-server (SWG/WSA) retourneert vervolgens een beschikbare UDP-poort naar de client om UDP-pakketten naar te sturen. Standaard is het 16000-16100. U kunt de poortnummers wijzigen.

De client begint vervolgens de UDP-pakketten die moeten worden doorgestuurd naar de nieuwe UDP-poort die beschikbaar is op de SOCKS5-server. SOCKS5-server stuurt deze UDP-pakketten door naar de externe server en stuurt de UDP-pakketten die van de externe server komen, terug naar de pc.

Wanneer u de verbinding wilt beëindigen, stuurt de pc een FIN-pakket via TCP. De SOCKS5-server beëindigt vervolgens de UDP-verbinding die voor de client is gemaakt en beëindigt

vervolgens de TCP-verbinding.



Waarschuwing: de informatie in dit document is gemaakt van de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

SOCKS Proxy-configuratie op SWA/WSA

U kunt navigeren naar Security services > SOCKS proxy om de SOCKS control poort en UDP request poorten te configureren. Dit maakt het ook mogelijk om de timeouts te configureren.

1. SOCKS versie 5 wordt ondersteund. Versie 4 wordt niet ondersteund.
2. Het SOCKS-protocol ondersteunt alleen directe voorwaartse verbindingen, zodat het geen omleidingen kan ondersteunen.
3. De SOCKS proxy ondersteunt geen upstream proxy's, zodat u het WSA socks-verkeer niet naar een andere upstream proxy kunt sturen. U moet altijd het beleid voor directe verbinding-routing gebruiken.
4. U kunt geen gebruik maken van de WSA functies zoals scannen, AVC, DLP en malware detectie.
5. Het beleidsspoor kan niet werken met socks proxy.
6. Er is geen SSL-decryptie-ondersteuning beschikbaar als verkeerstunnels van client naar server.
7. Socks proxy ondersteunt alleen basisverificatie.

Aanvullende informatie

Standaard wordt de DNS-resolutie lokaal gemaakt wanneer u SOCKS-verkeer via Firefox probeert te verzenden, waardoor de WSA geen hostnaam ziet in rapportage- of toegangslogboeken. Als we Remote DNS in Firefox inschakelen dan kan WSA DNS-resolutie doen en kunnen we de hostnaam bekijken in rapportage-/toegangslogboeken. De Remote DNS optie is beschikbaar in de nieuwste Firefox-versies. Als de optie niet beschikbaar is, probeert u deze stappen.

ongeveer:configuratie

Zoek Voorkeursnaam: proxy, vind network.proxy.socks_remote_dns en stel het in op True.

De browser van Google Chrome voert standaard DNS resolutie op de volmacht SOCKS uit zodat geen veranderingen nodig zijn.

In overeenstemming met het ondersteuningsdocument voor Google-chroom Proxy wordt SOCKSv5 alleen gebruikt om op TCP gebaseerde URL-verzoeken te proxy. Het kan niet worden gebruikt om UDP-verkeer door te geven.

Referentie

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

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.