Configurazione ed esame del proxy SOCKS su Secure Web Appliance

Sommario

Introduzione

Questo documento descrive il funzionamento del proxy SOCKS su Cisco SWA e fornisce una panoramica di come instrada il traffico tra un client e il server finale

Funzionamento del proxy SOCKS ad alto livello

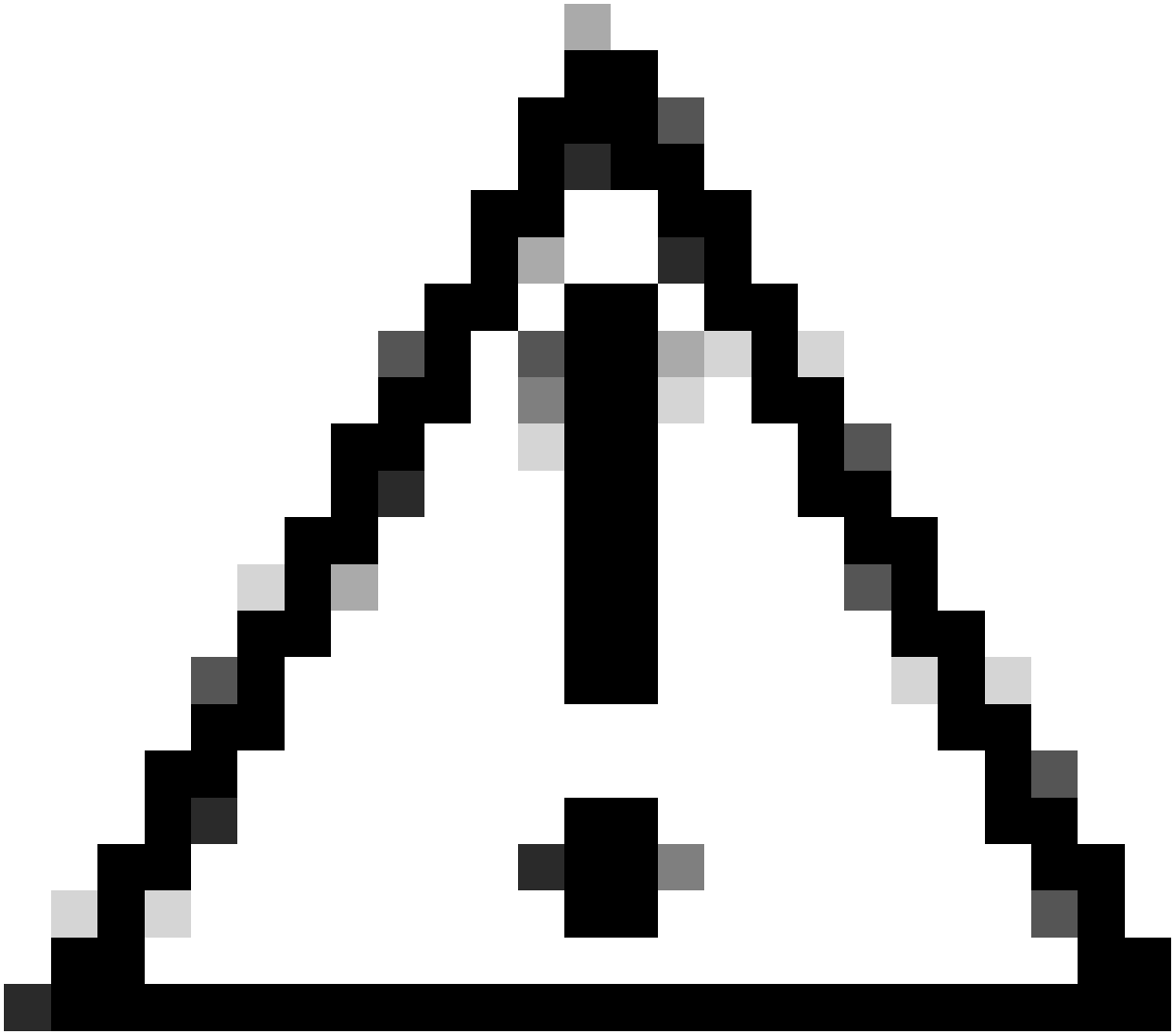
Socket Secure (SOCKS) è un protocollo di rete che facilita la comunicazione con i server tramite un proxy SOCKS (in questo caso SWA/WSA) instradando il traffico di rete al server effettivo per conto di un client. SOCKS è progettato per instradare qualsiasi tipo di traffico a livello di applicazione generato da qualsiasi programma.
Per impostazione predefinita, l'SWA utilizza la porta TCP 1080 per ascoltare il traffico SOCKS del client. I client possono configurare l'invio del traffico socks a WSA sulla porta TCP 1080. Se necessario, è possibile aggiungere altri numeri di porta.

SOCKS versione 5 supporta anche il tunneling UDP in modo che il client possa utilizzare anche la porta UDP per inviare il traffico al proxy. Per impostazione predefinita, è 16000-16100.

Per inoltrare un traffico UDP sul proxy SOCKS5, il client effettua una richiesta di associazione UDP sulla porta di controllo TCP 1080. Il server SOCKS5 (SWG/WSA) restituisce quindi al client una porta UDP disponibile a cui inviare i pacchetti UDP. Per impostazione predefinita, è 16000-16100. È possibile modificare i numeri di porta.

Il client inizia quindi a inviare i pacchetti UDP che devono essere inoltrati alla nuova porta UDP disponibile sul server SOCKS5. Il server SOCKS5 reindirizza questi pacchetti UDP al server remoto e reindirizza i pacchetti UDP provenienti dal server remoto al PC.

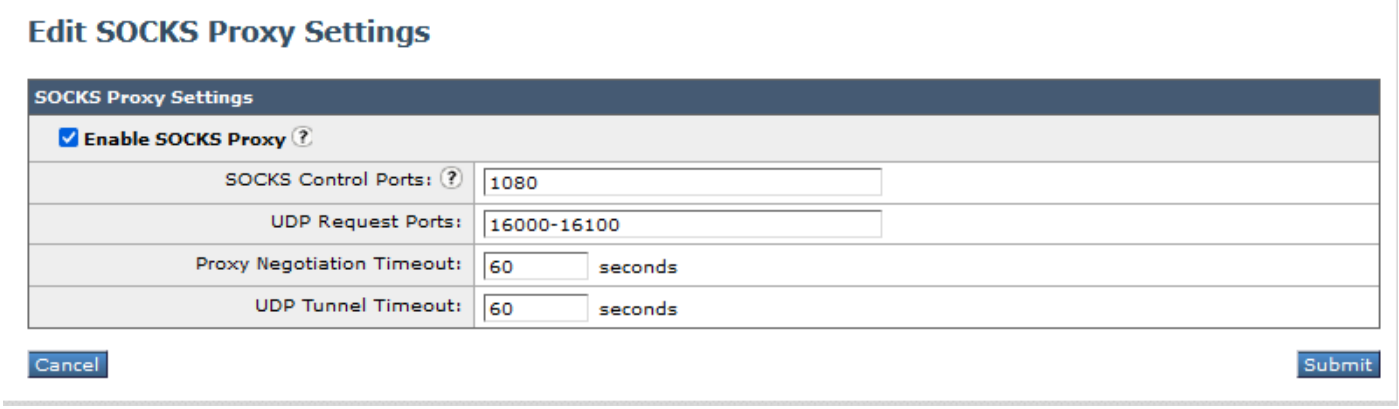
Quando si desidera terminare la connessione, il PC invia un pacchetto FIN tramite TCP. Il server SOCKS5 interrompe quindi la connessione UDP creata per il client e quindi la connessione TCP.



Attenzione: le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

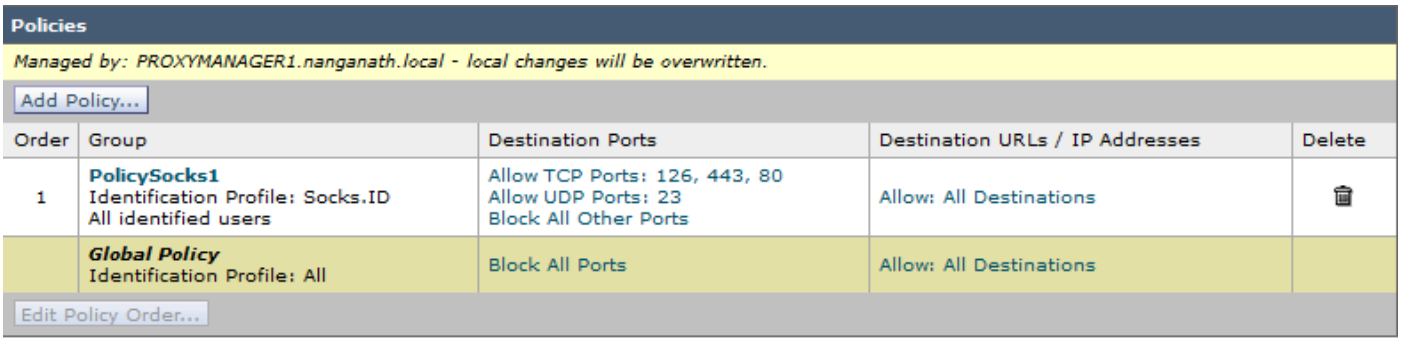
Configurazione proxy SOCKS su SWA/WSA

È possibile passare a Servizi di sicurezza > proxy SOCKS per configurare la porta di controllo SOCKS e le porte di richiesta UDP. Ciò consente anche di configurare i timeout.



È possibile configurare i criteri SOCKS selezionando Web Security Manager > SOCKS Proxy.

È possibile configurare i criteri in base alle esigenze e consentire porte TCP/UDP specifiche in base alle esigenze



Risoluzione dei problemi relativi al proxy SOCKS

È possibile visualizzare i log tramite tracciamento Web nella sezione SOCKS del modulo di report WSA o tramite i log degli accessi.

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,-,"-"-,"-,"-,"-,-,-,"-"-,-,-,"-,"-,-,-> - [Dettagli richiesta: ID = 2428020, Agente utente = -, Appartenenze a gruppi AD = (NESSUNO) -] ; "19/Maggio/2020 2:09:07:22 +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,-,"-","-"-,-,"-,-,-,-,-"-,-,-> - [Dettagli richiesta: ID = 2428030, Agente = -, Appartenenze al gruppo AD = (NONE) -]; "19/May/2022:09:07:22 +0530", IP server = 151.101.130.219

Non supportato nell'implementazione SWA SOCKS

1. SOCKS versione 5 è supportato. Versione 4 non supportata.
2. Il protocollo SOCKS supporta solo connessioni di inoltro diretto, quindi non può supportare reindirizzamenti.
3. Il proxy SOCKS non supporta i proxy upstream, quindi non è possibile inviare il traffico socks WSA a un altro proxy upstream. È sempre necessario utilizzare il criterio di routing della connessione diretta.
4. Non è possibile utilizzare le funzionalità WSA quali scansione, AVC, DLP e rilevamento malware.
5. La traccia dei criteri non può funzionare con il proxy SOCKS.
6. Non è disponibile alcun supporto per la decrittografia SSL come tunnel di traffico da client a server.
7. Il proxy Socks supporta solo l'autenticazione di base.

Ulteriori informazioni

Per impostazione predefinita, quando si tenta di inviare il traffico SOCKS tramite Firefox, la risoluzione DNS viene eseguita localmente, pertanto il WSA non visualizza alcun nome host nei report o nei log di accesso. Se si abilita il DNS remoto su Firefox, WSA può eseguire la risoluzione DNS e visualizzare il nome host nei registri di accesso/creazione rapporti. L'opzione DNS remoto è disponibile nelle versioni più recenti di Firefox. Se non è disponibile, eseguire la procedura seguente.

informazioni su:config
Nome preferenza di ricerca : proxy, trovare network.proxy.socks_remote_dns e impostarlo su True.

Per impostazione predefinita, il browser Google Chrome esegue la risoluzione DNS sul proxy SOCKS in modo che non siano necessarie modifiche.

Come indicato nel documento di supporto del proxy Google chrome, SOCKSv5 è utilizzato solo per le richieste di URL basate su TCP. Non può essere utilizzato per inoltrare il traffico UDP.

Riferimento

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

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).