Wat is inlogd in toegangslogboek voor HTTPS verkeer?

Inhoud

Bijgedragen door Kei Ozaki en Siddharth Rajpathak, Cisco TAC-engineers.

Vraag:

Wat is inloggen voor HTTPS-verkeer?

Milieu: Cisco Web Security Appliance (WSA) met AsyncOS-versies 7.1.x en hoger, HTTPS-proxy ingeschakeld

De manier waarop Cisco Web Security Appliance (WSA) HTTPS-verkeer logt, is anders dan normaal HTTP-verkeer. HTTPS-vermeldingen die zijn opgenomen in de toegangsdocumenten zullen er anders uitzien, afhankelijk van de manier waarop het verzoek is behandeld. In het algemeen heeft het andere kenmerken dan normaal HTTP-verkeer.

Wat wordt vastgelegd zal afhangen van welke implementatiemodus u gebruikt (expliciete voorwaartse modus of transparante modus).

Laten we eerst eens kijken naar een paar sleutelwoorden die je helpen om toeganglogs gemakkelijk te lezen.

TCP_CONNECT - Dit toont aan dat het verkeer op transparante wijze is ontvangen (via WCCP of L4 redirect ...enz.)
CONNECT - dit toont dat het verkeer expliciet is ontvangen
DECRYPT_WBRS - dit toont aan dat WSA heeft besloten het verkeer te decrypteren vanwege WBRS-score
PASSTHRU_WBRS - Dit toont aan dat WSA heeft besloten door het verkeer te passeren door WBRS-score
DROP_WBRS - Dit toont aan dat WSA heeft besloten het verkeer te laten vallen vanwege WBRS-score

- Wanneer **HTTPS** verkeer wordt gedecrypteerd, zal WSA twee ingangen registreren.
- **TCP_CONNECT** of **CONNECT**, afhankelijk van het type verzoek dat wordt ontvangen en **"GET https://"** die de gedecrypteerde URL toont.
- Full **URL** zal alleen zichtbaar zijn als WSA het verkeer decrypteert.

Let ook op:

- In de transparante modus wordt alleen het IP-adres van de bestemming oorspronkelijk weergegeven
- In de expliciete modus zal WSA de bestemming hostname zien

Hieronder zie je wat voorbeelden van wat je zag bij e-mails:

Transparent - decrypteren
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 TCP_CONNECT tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - DECRYL WBRS-DefaultGroup-test.id-NONE-NONE-Default-routing <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543171.166 395 192.168.30.103 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/192.168.34.3 2 afbeelding/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0-,-,--,-,-,-,-,-,-,-,-,-,-,-,-> -
Transparante passeren
1252543337.373 690 192.168.30.103 TCP_MISS/20044 TCP_CONNECT tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - ASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Transparante - Drop
1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - DROP_WBRS - DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,-9.1.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,--,-> -
Expliciet - decrypteren
25254358.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/2000 40 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE -Default routing <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543559.535 1127 10.66.71.105 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/www.example.com image/gif DEFAULT_CASE-test.policy-test.id - NIET-NONE <Sear,5.0,0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-
Expliciet - doorvoer
1252543491.302 568 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - PASSTHRU_WBRS-DefaultGroup-test.id NONE-NONE-Default routing <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Expliciet - Drop
1252543668.375 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - NONE/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE <SEAR-N, 9,1,-,-,-,-,-,-,-,-,-,