Che cos'è registrato nel log degli accessi per il traffico HTTPS?

Sommario

Domanda:

Contributo di Kei Ozaki e Siddharth Rajpathak, tecnici Cisco TAC.

Domanda:

Che cos'è registrato nel log degli accessi per il traffico HTTPS?

Ambiente: Appliance Cisco Web Security (WSA) con AsyncOS versione 7.1.x e successive, proxy HTTPS abilitato

Il modo in cui Cisco Web Security Appliance (WSA) registra il traffico HTTPS è diverso dal normale traffico HTTP. Le voci HTTPS registrate nei log degli accessi avranno un aspetto diverso a seconda di come è stata gestita la richiesta. In generale ha caratteristiche diverse rispetto al normale traffico HTTP.

Il contenuto registrato dipende dalla modalità di distribuzione utilizzata (modalità di inoltro esplicito o modalità trasparente).

Esaminiamo innanzitutto alcune parole chiave che semplificano la lettura dei log degli accessi.

TCP_CONNECT: visualizza il traffico ricevuto in modo trasparente (tramite WCCP o reindirizzamento L4 ...ecc.)
CONNECT - indica che il traffico è stato ricevuto esplicitamente
DECRYPT_WBRS - Questo messaggio mostra che WSA ha deciso di decrittografare il traffico a causa del punteggio WBRS
PASSTHRU_WBRS - Questo mostra che WSA ha deciso di passare attraverso il traffico a causa del punteggio WBRS
DROP_WBRS: indica che WSA ha deciso di interrompere il traffico a causa del punteggio WBRS

- Quando il traffico **HTTPS** viene decrittografato, WSA registra due voci.
- **TCP_CONNECT** o **CONNECT** a seconda del tipo di richiesta ricevuta e **"GET https://"** che indica l'URL decrittografato.
- L'**URL** completo sarà visibile solo se WSA decrittografa il traffico.

Si noti inoltre che:

- In modalità trasparente, WSA vedrà solo l'indirizzo IP di destinazione inizialmente

- In modalità esplicita, WSA vedrà il nome host di destinazione

Di seguito sono riportati alcuni esempi di quanto è possibile visualizzare nei log degli accessi:

Trasparente - Decrittografa
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/2000 TCP_CONNECT tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,- > - 1252543171.166 395 192.168.30.103 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/192.168.34.32 image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE <Sear,5.0,0,-,-,-,-,-,- -,-,-,-> -
Trasparente - Passthrough
125254337.373 690 192.168.30.103 TCP_MISS/200 2044 TCP_CONNECT tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,- -,-,-> -
Trasparente - Elimina
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,-,-,-,-,-,-> -
Esplicito - Decrittografa
25254358.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/20040 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-> - 125254359.535 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-NONE-NONE <Sear,5.0,0,-,-,-,0,-,-,-,-,-,-,-> -
Esplicito - Pass-through
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-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-> -
Esplicito - Elimina
125254368.375 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - NONE/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-,-> -