Que é log entrado do acesso para o tráfego HTTPS?

Índice

Contribuído por Kei Ozaki e por Siddharth Rajpathak, engenheiros de TAC da Cisco.

Pergunta:

Que é log entrado do acesso para o tráfego HTTPS?

Ambiente: Versões 7.1.x e mais recente sendo executado de AsyncOS da ferramenta de segurança da Web de Cisco (WSA), proxy HTTPS permitido

O tráfego dos logs HTTPS da ferramenta de segurança da Web de Cisco da maneira (WSA) é diferente comparado ao tráfego de HTTP normal. As entradas HTTPS gravadas nos accesslogs olharão diferentes segundo como o pedido foi tratado. No general tem as características diferentes comparadas ao tráfego de HTTP normal.

O que é registrado dependerá de que modo do desenvolvimento você está usando (modo ou modo transparente dianteiro explícito).

Deixe-nos primeiramente olhar algumas palavras-chaves que o ajudariam acesso de leitura registra facilmente.

TCP_CONNECT - isto mostra que o tráfego esteve recebido transparentemente (através do WCCP ou do L4 reoriente… etc.)
CONECTE - isto mostra que o tráfego esteve recebido explicitamente
DECRYPT_WBRS - isto mostra que WSA decidiu decifrar o tráfego devido à contagem WBRS
PASSTHRU_WBRS - isto mostra que WSA decidiu passar com o tráfego devido à contagem WBRS
DROP_WBRS - isto mostra que WSA decidiu deixar cair o tráfego devido à contagem WBRS

- Quando o tráfego **HTTPS** é decifrado, WSA registrará duas entradas.
- **TCP_CONNECT** ou **CONECTAM** segundo o tipo de pedido que estão sendo recebidos e de **"GET https://" que** mostra a URL decifrada.
- **A URL** completa será somente visível se WSA decifra o tráfego.

Por favor igualmente note isso:

- No modo transparente, WSA verá somente o endereço IP de destino inicialmente

- No modo explícito, WSA verá o nome de host de destino

Estão abaixo alguns exemplos do que você veria nos accesslogs:

Transparente - Decrypt
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 0 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 imagem/GIF DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
Passagem transparente
1252543337.373 690 192.168.30.103 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,-,-,-,-,-,-,-,-,-,-,-,-> -
Transparente - Gota
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,-,-,-,-,-,-,-,-,-,-,-,-> -
Explícito - Decrypt
252543558.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 CONECTAM tunnel://www.example.com:443/ - www.example.com DIRETO - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543559.535 1127 10.66.71.105 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - imagem DIRETA de www.example.com/GIF DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
Explícito - Passe completamente
1252543491.302 568 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256 CONECTAM tunnel://www.example.com:443/ - www.example.com DIRETO - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-> -
Explícito - Gota
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 CONECTA tunnel://www.example.com:443/ - NENHUNS - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-> -