HTTPS トラフィックのアクセス ログには何が記録されますか。

目次

著者：Cisco TAC エンジニア、Kei Ozaki および Siddharth Rajpathak

質問：

HTTPS トラフィックのアクセス ログにはどのような情報が記録されますか

環境： AsyncOS バージョン 7.1.x 以降が稼働し、HTTPS プロキシが有効に設定されている Cisco Web セキュリティ アプライアンス（WSA）

Cisco Web セキュリティ アプライアンス（WSA）による HTTPS トラフィックのログ記録方法は、通常の HTTP トラフィックとは異なります。 アクセス ログに記録される HTTPS エントリは、リクエストの処理方法に応じて異なります。 一般に、HTTPS トラフィックの特性は、通常の HTTP トラフィックとは異なります。

記録される情報は、使用している導入モード（明示的順方向モードまたはトランスペアレント モード）によって異なります。

まず、アクセス ログの内容を理解する上で役立ついくつかのキーワードを説明します。

TCP_CONNECT：トラフィックが（WCCP または L4 リダイレクトなどを経由して）透過的に受信されたことを示します。
CONNECT：トラフィックが明示的に受信されたことを示します。
DECRYPT_WBRS：WSA が、WBRS スコアに基づきトラフィックを復号することに決定したことを示します。
PASSTHRU_WBRS：WSA が、WBRS スコアに基づきトラフィックをパススルーすることに決定したことを示します。
DROP_WBRS：WSA が、WBRS スコアに基づきトラフィックをドロップすることに決定したことを示します。

- **HTTPS** トラフィックが復号されると、WSA は 2 つのエントリをログに記録します。
- 受信する要求のタイプに応じて **TCP_CONNECT** または **CONNECT** と、復号された URL を示す「**GET https://**」。
- WSA がトラフィックを復号する場合、全体の **URL** だけが表示されます。

また、次のことに注意してください。

- トランスペアレント モードでは、最初に WSA は宛先 IP アドレスだけを認識します。
- 明示的モードでは、WSA は宛先ホスト名を認識します。

アクセス ログに表示される情報の例を次に示します。

トランスペアレント：復号
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 image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
トランスペアレント：パススルー
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,-,-,-,-,-,-,-,-,-,-,-,-> -
トランスペアレント：ドロップ
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,-,-,-,-,-,-,-,-,-,-,-,-> -
明示的：復号
252543558.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - 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 - DIRECT/www.example.com image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
明示的：パススルー
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,-,-,-,-,-,-,-,-,-,-,-,-> -
明示的：ドロップ
1252543668.375 1 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,-,-,-,-,-,-,-,-,-,-,-,-> -