HTTPS流量的訪問日誌中記錄了哪些內容？

目錄

問題：

作者：Kei Ozaki和Siddharth Rajpathak，思科TAC工程師。

問題：

HTTPS流量的訪問日誌中記錄了哪些內容？

環境:運行AsyncOS版本7.1.x及更高版本的思科網路安全裝置(WSA)，啟用HTTPS代理

思科網路安全裝置(WSA)記錄HTTPS流量的方式與常規HTTP流量不同。 根據請求處理方式，訪問日誌中記錄的HTTPS條目將有所不同。通常，與正常HTTP流量相比，它具有不同的特徵。

所記錄的內容取決於您使用的部署模式（顯式轉發模式或透明模式）。

首先讓我們看一些能幫助您輕鬆讀取訪問日誌的關鍵字。

TCP_CONNECT -這顯示流量是以透明方式接收的(透過WCCP或L4重新導向……等等)
CONNECT — 這顯示流量是明確接收的
DECRYPT_WBRS — 這顯示WSA已決定由於WBRS得分而解密流量
PASSTHRU_WBRS — 這顯示WSA已決定由於WBRS分數而傳遞流量
DROP_WBRS — 這顯示WSA已決定由於WBRS得分而丟棄流量

- HTTPS流量解密時，WSA將記錄兩個條目。
- TCP_CONNECT或CONNECT（取決於接收的請求型別）和「GET https://」顯示解密URL。
- 只有在WSA解密流量時，才能看到完整的URL。

另請注意：

- 在透明模式下，WSA最初只會看到目標IP地址
- 在顯式模式下，WSA將看到目標主機名

以下是您在訪問日誌中看到的內容的一些示例：

透明 — 解密
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,-,-,-,-,-,0,0,0,-,-

透明 — 直通

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,-,-,-,-,-,-,-,-> -

透明 — 丟棄

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,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-

顯式 — 解密

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,-,-,-,-,-,-> -

顯式 — 通過

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,-,-,-,-,-,-,-,-,-,-,-,-> -

顯式 — 丟棄

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,-,-,-,-,-,-,-,-,-,-,-,-> -