瞭解Secure Web Appliance中的HTTPS訪問日誌格式

目錄

簡介

本檔案介紹適用於HTTPS流量的安全網路裝置(SWA)存取記錄。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝物理或虛擬SWA。
- 許可證已啟用或已安裝。
- 安全殼層(SSH)使用者端。
- 安裝嚮導已完成。
- 對SWA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

與普通HTTP流量相比，訪問日誌中的Cisco SWA HTTPS流量記錄的方式不同。

附註：日誌取決於代理部署模式，在顯式轉發模式或透明模式中，日誌是不同的。

訪問日誌中的關鍵字

以下是您在訪問日誌中可以看到的一些重要關鍵字：

TCP_CONNECT :這顯示流量是以透明方式接收的（透過WCCP、L4重新導向或其他透明重新導向方法）
連線:這顯示流量是明確接收的。
DECRYPT_WBRS :這顯示SWA已根據Web信譽得分(WBRS)得分解密流量。
PASSTHRU_WBRS :這顯示由於WBRS得分，SWA已通過流量。
DROP_WBRS :這顯示SWA已因WBRS得分而丟棄流量

訪問日誌中的HTTPS日誌

HTTPS流量解密時，WSA會記錄兩個條目。

- TCP_CONNECT tunnel://或CONNECT tunnel://取決於收到的請求型別，這表示流量已加密（尚未解密）。
- GET https://顯示已解密的URL。

附註：僅當SWA解密流量時，透明模式中的完整URL才可見。

```
1706174571.215 582 10.61.70.23 TCP_MISS_SSL/200 39 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e
1706174571.486 270 10.61.70.23 TCP_MISS_SSL/200 1106 GET https://www.example.com:443/ - DIRECT/www.exam
```

附註：在透明模式下，當流量重定向至SWA時，SWA最初具有目標IP地址。

以下是您在訪問日誌中看到的內容的一些示例：'

透明部署 — 解密的流量
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 0 TCP_CONNECT 192.168.34:443/ - DIRECT/192.168.34.32 - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <A 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,-,-
透明部署 — 直通流量
1252543337.373 690 192.168.30.103 TCP_MISS/200 2044 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <A sear，9.0,-,-,-,-,-,-,-,-,-,-,-,->
透明部署 — 丟棄
1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <A sear、-9.1.0、-、-、-、-、-、-、-、-、-、-、-、-、-、-、-、->
顯式部署 — 解密的流量
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,-,-,-,-> -
顯式部署 — 直通流量
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,-,-,-,-,-,-,-,-,-,-,-,-,-,-
顯式部署 — 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,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -

相關資訊

- 思科安全Web裝置AsyncOS 15.0使用手冊 — LD（有限部署） — 故障排除……
- 配置訪問日誌中的效能引數 — Cisco

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。