Secure Web ApplianceのHTTPSアクセスログ形式について

内容

はじめに

このドキュメントでは、HTTPSトラフィックのセキュアWebアプライアンス(SWA)アクセスログについて説明します。

前提条件

要 件

次の項目に関する知識があることが推奨されます。

- 物理または仮想SWAがインストールされている。
- ライセンスがアクティブ化またはインストールされていること。
- セキュアシェル(SSH)クライアント。
- セットアップウィザードが完了しました。

- SWAへの管理アクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

アクセスログに記録されるCisco SWA HTTPSトラフィックの方法は、通常のHTTPトラフィックとは異なります。

注：ログはプロキシ導入モードによって異なり、明示的転送モードまたは透過モードではログが異なります。

アクセスログのキーワード

アクセスログに表示される重要なキーワードを次に示します。

TCP_CONNECT（オプション）：トラフィックが透過的に（WCCP、L4リダイレクト、またはその他の透過的なリダイレクション方式を介して）受信されたことを示します。
CONNECT（オプション）：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（任意）:SWAが、Webレピュテーションスコア(WBRS)スコアに基づいて、トラフィックを復号したことを示します。
PASSTHRU_WBRS:WBRSスコアにより、SWAがトラフィックをパススルーしたことが示されます。
DROP_WBRS:WBRSスコアによりSWAでトラフィックがドロップされたことを示します。

アクセスログのHTTPSログ

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。

- TCP_CONNECT tunnel://またはCONNECT tunnel://は、受信した要求のタイプによって異なります。つまり、トラフィックは暗号化されています（まだ復号化されていません）。
- GET https://は復号化されたURLを表示します。

注：トランスペアレントモードのフルURLは、SWAがトラフィックを復号する場合にのみ表示されます。

```
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.examp
```

注：トランスペアレントモードでは、トラフィックがSWAにリダイレクトされたときに、最初はSWAに宛先IPアドレスがあります。

アクセスログに表示される情報の例を次に示します。

透過的な導入：復号化されたトラフィック
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 0 TCP_CONNECT 192.168.34.32:443/ – 直接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,-,-,-,-,-,-,-> -
透過的な導入：パススルートラフィック
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 <Sear,Default 9.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> -
透過的な導入：ドロップ
1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT 192.168.34.32:443/ – 直接/19 2.168.34.32 - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,-9.1.0,-> -
明示的な導入：復号化されたトラフィック
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,-,-,-,-,-,-,-> -
明示的な導入：パススルートラフィック
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -
明示的な展開 – 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,-,-,-,-,-,-,-,-,-,-,-,-,-> -

関連情報

- AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド – LD（限定導入） – トラブルシューティング...
- アクセスログのパフォーマンスパラメータの設定 – Cisco

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。