SWAでの復号化レートの決定

内容

はじめに

このドキュメントでは、以前はWSAと呼ばれていたSecure Web Appliance(SWA)で復号化されたトラフィックの割合を計算する手順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。

- インストールされている物理または仮想のセキュアWebアプライアンス(SWA)。
- ライセンスの有効化またはインストール
- 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ました。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。

復号化のパフォーマンスへの影響

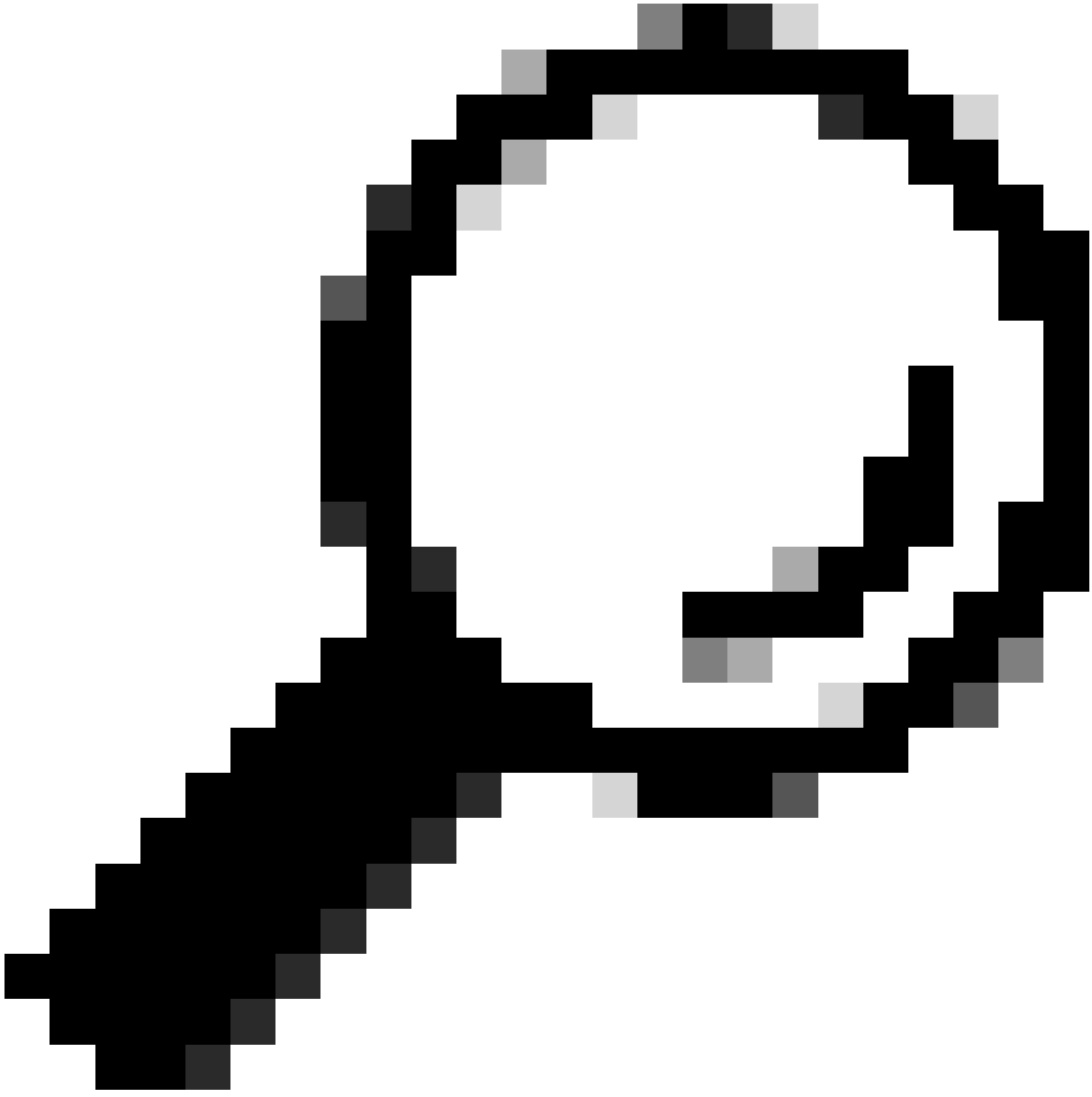
SWAによって実行されるすべてのサービスの中で、パフォーマンスの観点から見ると、Hypertext Transfer Protocol Secure(HTTPS)トラフィックの評価が最も重要です。

復号化されたトラフィックの割合は、アプライアンスのサイジング方法に直接影響します。管理者は、Webトラフィックの少なくとも75 %をHTTPSと見なすことができます。

最初のインストールの後、復号化されたトラフィックの割合を決定して、将来の成長に対する期待が正確に設定されるようにする必要があります。導入後は、四半期ごとにこの数を確認する必要があります。

復号化レートが30 %を超えており、SWAにパフォーマンスの問題がある場合は、次のいずれかを推奨します。

- さまざまなカテゴリまたは信頼できるURL（Microsoft Updateやウイルス対策の更新プログラムなど）の復号化ポリシーから復号化を削除する
- 負荷を分散するために、より多くのSWA間でロードバランシングを行う



ヒント:SWAで復号化をバイパスする方法の詳細については、

---

https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html を参照してください。

復号化率を計算する手順

すべてのHTTPSトラフィックと比較して、復号化されるHTTPSトラフィックの割合を見つけるには、SWAファイル転送プロトコル(FTP)からaccess_logsをコピーします。

この数値は、単純なBashコマンドまたはPowerShellコマンドを使用して取得できます。各環境について説明する手順を次に示します。

1. 合計HTTPS接続数を調べます（明示的および透過的の両方）。

```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length
```

2. 復号化されたHTTPS接続の数を確認します。

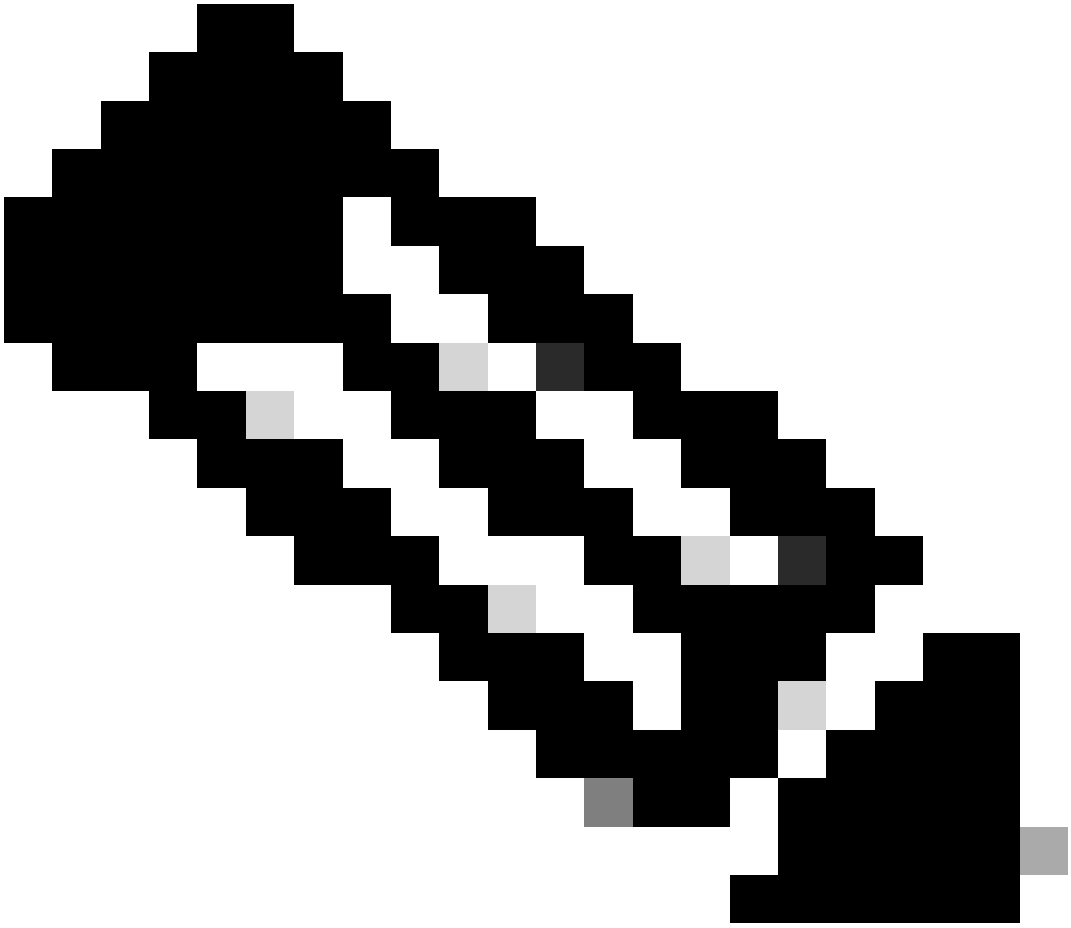
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT'| Select-String -Pattern 'DE
```

3. 2番目の値を1番目の値で除算し、100を乗算します。

CLIからの全体的なトラフィック統計情報

トラフィックの統計情報は、CLIでaccessloganalyzerコマンドを使用して表示できます。このコマンドでレポートの時間範囲または過去N時間を選択できます。



注：コマンドの実行時間は、選択した期間によって異なります。

```
SWA_CLI> accessloganalyzer

Choose the option to define the time range:
- HOURS - Last N hours.
- RANGE - Time range with start and end specified in  MM/DD/YYYY HH:MM:SS format.
[]> HOURS

Analyze logs upto N hours old (oldest on this WSA is N = 312 hours). Enter N:
[]> 10

The log processing might take more than 15 secs. Do you want to continue: (Yes/No)
[No]> yes



-------------------------------------------------------------------------------------------------
                                        HTTP                HTTPS               Cumulative
---------------------------------------- ------------------- ------------------- -------------------
Num transactions                        1512509             4170261             5682770
```

Transaction/sec	42	115	157
Bandwidth (Mbps)	0.0001	0.0004	0.0003
Max Resp time (ms)	643269	285036670	285036670
Average Resp time(ms)	95663	141715	129458
Max Object size (KB)	92246	1215832	1215832
Avg Object size (Total Trans)(KB)	5	54	41
Avg Object size (Allowed Trans) (KB)	20	67	62
Methods			
GET	1295658	0	1295658
POST	34968	0	34968
CONNECT	0	4170261	4170261
Others	181883	0	181883
Status Codes			
1xx	0	0	0
2xx	319799	3351382	3671181
3xx	75011	0	75011
4xx	11697	115467	127164
5xx	1105999	703412	1809411

関連情報

AsyncOSAsyncOSまたはCisco Cisco Web Applianceユーザガイド – LD(LimLDed Deployment) – シスコ

UCiscocure Webアプライアンスのベストプラクティス – シスコ

Ciscoセキュリティアプライアンス(WSA)での認証および復号化からのOffice 365トラフィックのシスコ免除(WSAco)

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。