SWG Webサイトアクセス問題のトラブルシューティング

内容

はじめに

このドキュメントでは、Umbrella Secure Web Gateway(SWG)プロキシで見られるWebサイトアクセスの問題をトラブルシューティングする方法について説明します。

背景説明

www.xyz.comのWebサイトにはSWGプロキシ経由でアクセスできず、ユーザがインターネットに直接アクセスしようとすると（Umbrella SWGが写真に含まれていない場合）、正常に機能すると仮定します。 SWG経由でWebサイトにアクセスできない場合に報告されるさまざまな症状やさまざまな種類のエラーメッセージを確認しましょう。最も一般的なものは、502の不正なゲートウェイ、502の「could not relay message upstream」エラー、アップストリーム証明書の失効、アクセス拒否403の禁止、アップストリーム暗号の不一致、Webサイトがしばらくの間回転した後にタイムアウトしたことです。

アップストリームブロックが原因の「Access Denied 403」エラー

Webサーバまたはアップストリーム側が、SWGプロキシの出力IP範囲をブロックまたはスロットリングしています。たとえば、Akamai WAFには、いくつかのSWG出力IP範囲がリストされたブロックがあります。この問題を解決するには、Webサイトの管理者に連絡し、IP範囲のブロック

を解除してもらうのが唯一の方法です。それまでは、AnyConnect SWGおよびPACファイルの導入に外部ドメイン管理リストを使用してSWGをバイパスします。つまり、このタイプの問題はプロキシ自体が原因ではなく、プロキシとWebサーバ間の互換性の問題が原因です。出力IPのブロックによる「Access Denied 403」エラー専用のKBを示すリンクを次に示します。

また、ここに記載されているリンクも、AkamaiがリストされたIPアドレスをブロックする理由のいくつかについて説明しています。

Javaの問題による「Access Denied 403」エラー

Webサイトにアクセスできず、ファイルインスペクション設定が有効なSWG MPSプロキシを介して要求が送信されると、「Access Denied or 403 Forbidden - Umbrella cloud security gateway error」がスローされます。ただし、ファイル検査を無効にすると、Webサイトは正常にロードされます。または、Webサイトをバイパス復号化すると、Webサイトは正常にロードされます。

問題の根本原因の概要

MPSでのJava関連の問題は何ですか。

プロキシがサーバへの接続を試行した後、問題のサイトまたはWebサーバは、SNIまたはSSLアラートに関するTLS警告をプロキシに返します。基本的に、これはclient helloが送信された後に発生します。設計上、MPSプロキシ（Javaなどに基づく）は、SNI解析中に、説明フィールドに「Unrecognized Name」が含まれるすべてのTLSアラートを エラーとして処理し、トランザクションを終了します。詳細はここを参照

これはSWGまたはMPSプロキシの問題ではないことに注意してください。これは、サーバ側の設定ミスが原因でSWGやその他のプロキシと互換性がない場合の1つです。通常、ブラウザはこの警告を無視しますが、SWGまたはその他のコンテンツセキュリティフィルタはSSL警告を致命的なエラーとして扱い、セッションを終了します。その結果、ユーザに対して403個の禁止されたエラーページが表示されます。また、502 Bad Gatewayエラーが報告される場合もありますが、この図に示すように、ほとんどの例では403 forbiddenエラーが表示されています。

15151734443924

MPSはアプリケーション層で動作するため、TLSプロトコルで生成されるアラートに基づいてTLS層がトランザクションを処理する方法はほとんど、あるいはまったく制御できません。TLSエンドポイント/証明書が正しく設定されていることを確認するのは、サーバの責任です。こちらのリンクを参照してください。

問題を絞り込んだりトラブルシューティングしたりするには、SSLラボから簡単に指摘できます。

15152060146964

SWGプロキシを使用せずにWebサイトにアクセスする場合、またはSWGからのHTTPSインスペクションをバイパスする場合、Webサイトは機能します。これは、ブラウザがSNI Unrecognized nameアラートを無視し、Webサーバとの通信を続行するためです。

この記事を書いている時点で、推奨される回避策はシスコが皆様に提案できる最善の緩和策です。近い将来、新しいプロキシアーキテクチャを使用すると、これらの問題により適切に対処できるようになります。

解決方法

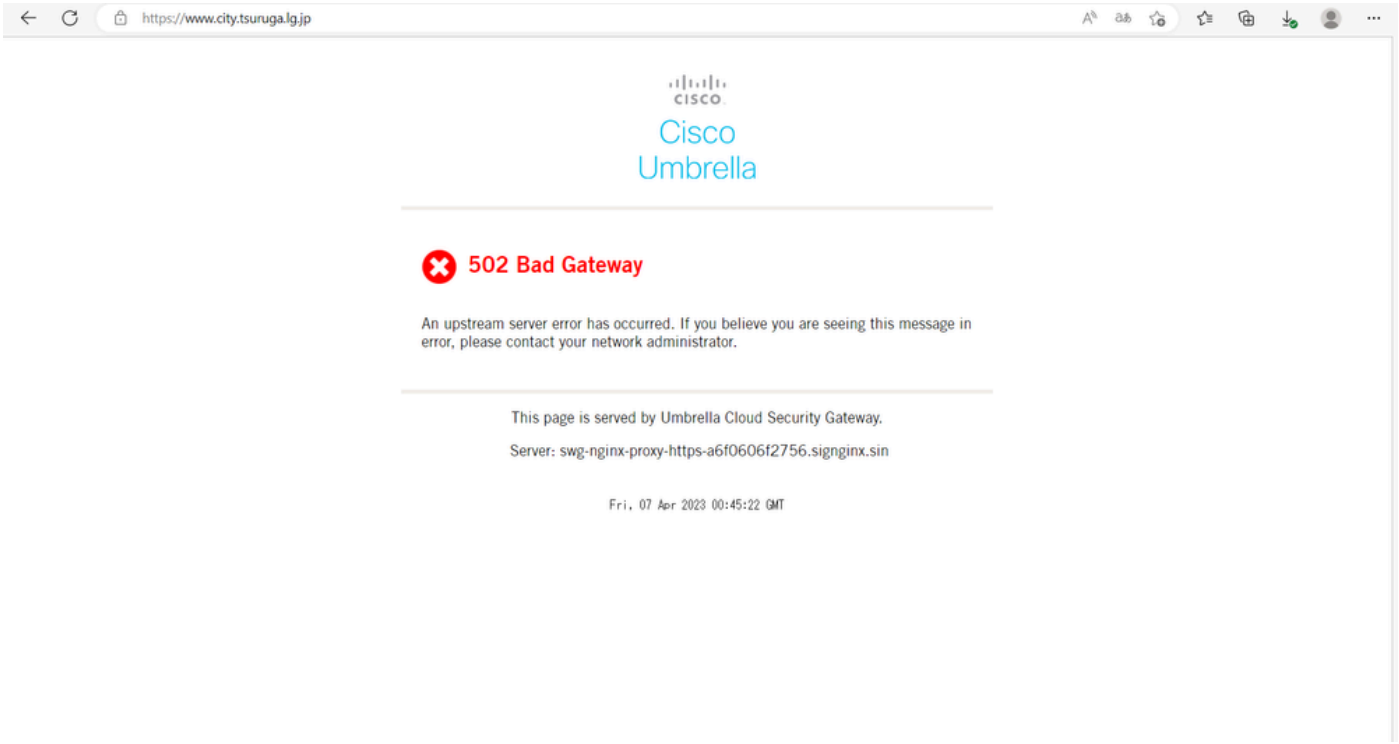
1. 影響を受けるドメインの復号化を無効にする – または
2. 宛先リストにドメインを追加し、許可ルールを関連付けます（サイトを信頼する場合）

502不良ゲートウェイとは何ですか。

502 Bad Gateway Errorは、サーバがゲートウェイまたはプロキシとして動作していて、アップストリームサーバから無効な応答を受信したことを意味します。ユーザがSWGプロキシ経由でWebサイトにアクセスしようとすると、2つの通信フローが発生します。

a)クライアント – >プロキシ接続（ダウンストリーム）
b)プロキシ – >Webサーバ接続の終了（アップストリーム）

502 Bad Gateway」エラーがSWGプロキシ(MPS、Nginx)とエンドサーバ接続の間で発生。



15026978020884

502不良ゲートウェイの一般的な要因

1. サポートされていないSWG暗号スイート

2. クライアント証明書認証要求

3. SWGプロキシによって追加または削除されるヘッダー

サポートされていないSWG暗号スイート

TLSネゴシエーション中に、サポートされていないSWG暗号スイートをWebサーバが報告したと仮定します。SWG MPS（モジュラプロキシサービス）プロキシは、TLS_CHACHA20_POLY1305_SHA256暗号スイートをサポートしていないことに注意してください。SWGがサポートする暗号スイートとTLSについては別の記事があることにご注意ください。client helloおよびserver helloでの暗号スイートの交換中にキャプチャされたその他のパケットを確認することで、この問題を簡単に特定できます。トラブルシューティングの手順として、特定の暗号を使用するように強制するCURLコマンドを使用して問題を絞り込み、例1と2に示すように暗号スイートが原因であることを確認します。

Curlコマンドの例:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
 - curl -x  proxy.sig.umbrella.com:80 -v  xyz.com:80
```

```
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Testing website without Proxy

```
: - curl -v www.xyz.com:80
```

Mac/Linux:

```
  - curl -vvv -o /dev/null -k -L www.cnn.com
```

Windows:

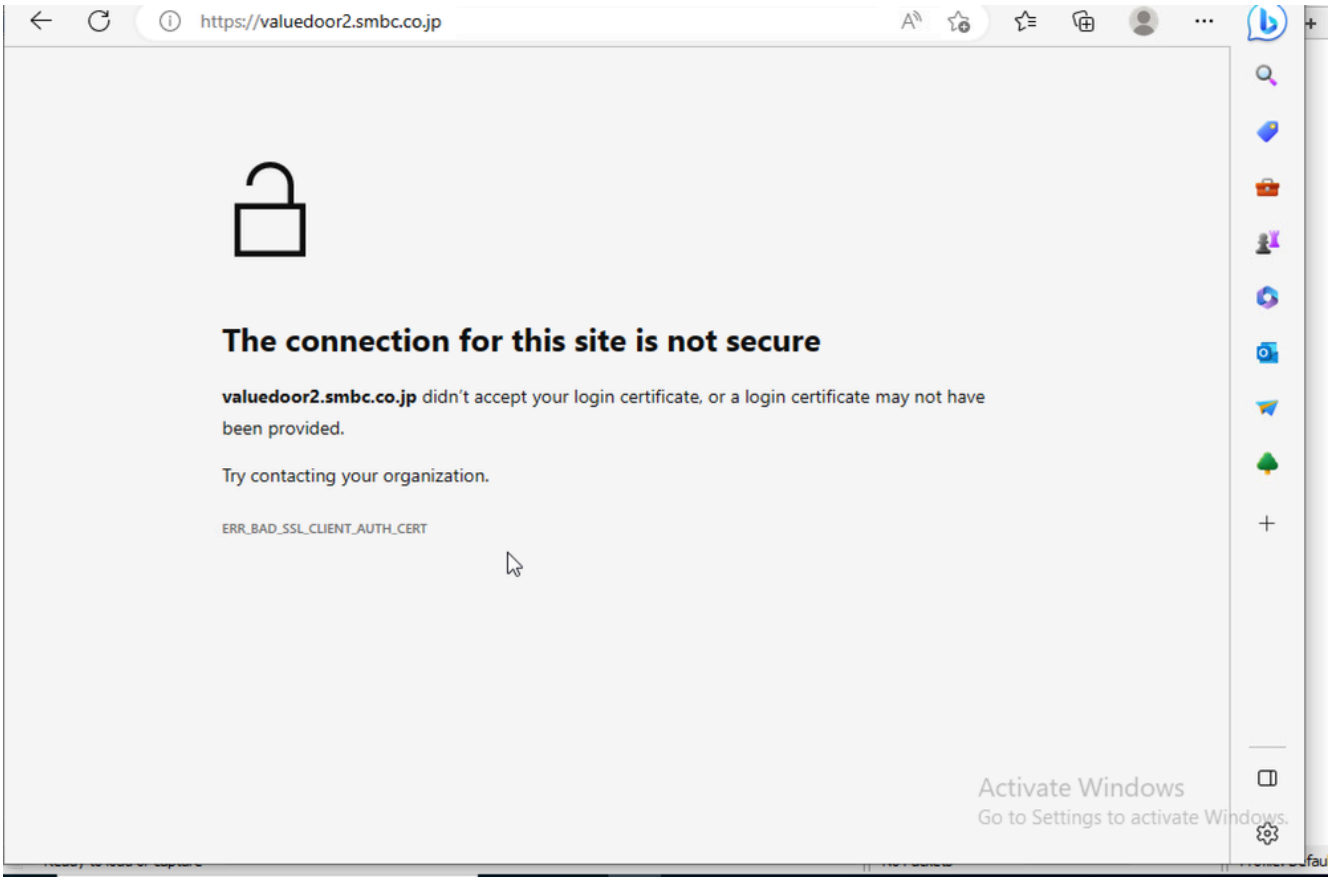
```
 - curl -vvv -o null -k -L www.cnn.com
```

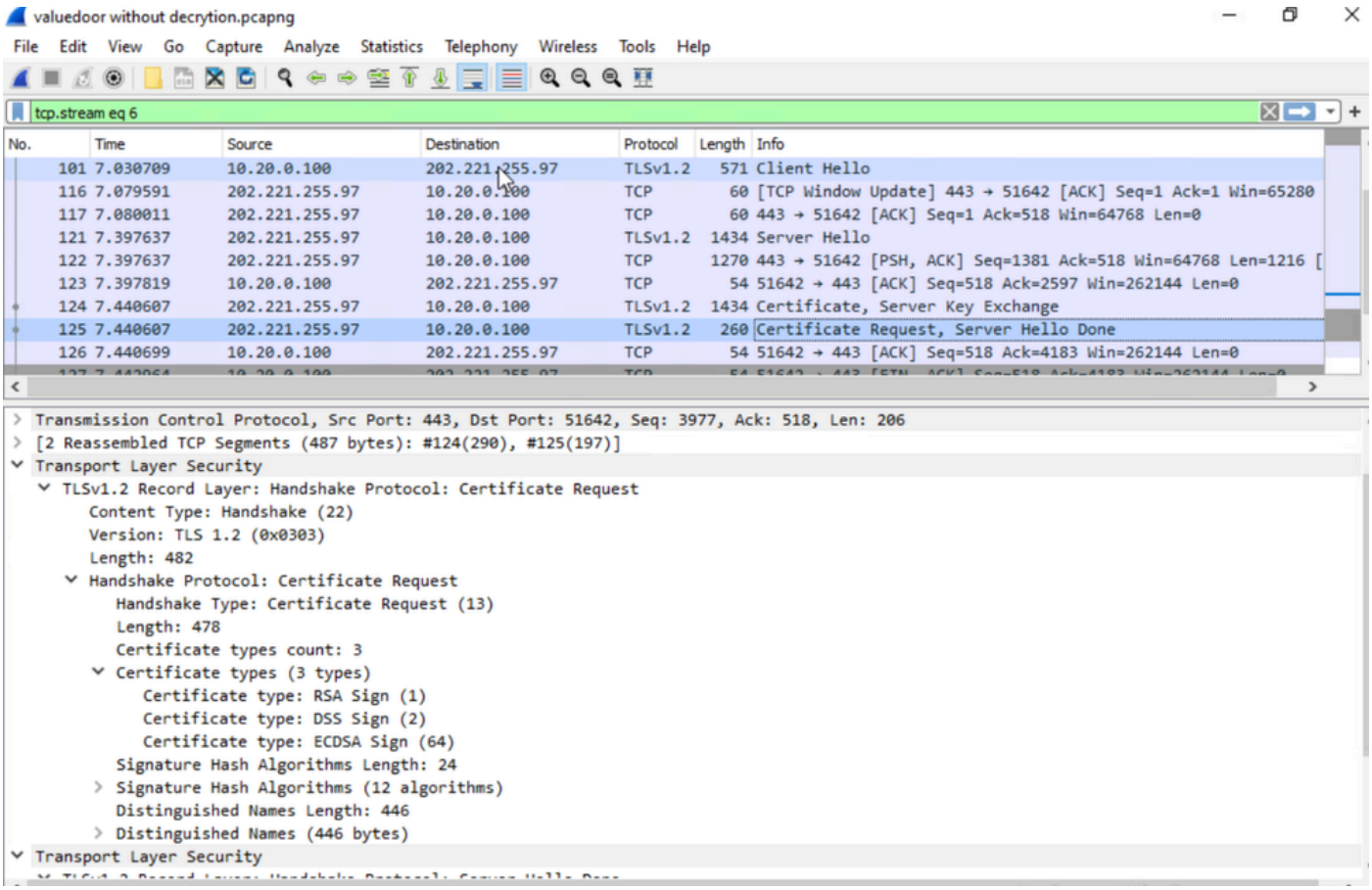
解決方法

この問題を解決するには、選択的な復号化リストを使用して、問題のあるWebサイトの検査をスキップします。

クライアント証明書認証要求

SWGプロキシとアップストリーム間のTLSハンドシェイク中、アップストリームWebサーバはクライアント証明書認証を想定します。クライアント証明書認証がサポートされていないため、外部ドメイン管理リストを使用してプロキシからこれらのドメインをバイパスする必要があります。httpsインスペクションだけをバイパスするだけでは不十分です。例：https://valuedoor2.smbc.co.jp

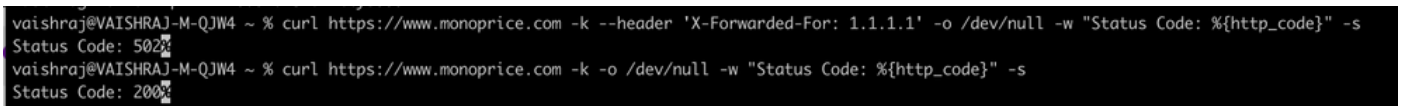




15027192992276

プロキシによって追加されたヘッダー

HTTPSインスペクションが有効な場合、Webサーバは、SWGプロキシによって追加されたX-Forward-For(XFF)ヘッダーが原因で502 bad gateway(NG)エラーを報告しています。MPSプロキシを使用したファイルスキャンの問題を除外するために、最初にhttpsインスペクションを使用する場合と使用しない場合の問題のトラブルシューティングを行うことで、502の不良ゲートウェイの問題の大部分を簡単に絞り込むことができます。



15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_co
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

HTTPSインスペクションがオンの場合はXFFヘッダーを使用します。これにより、アップストリームサーバはクライアントIP（ユーザの物理的な場所）に基づいて最適な位置情報コンテンツを提供できます。

HTTPSインスペクションが有効になっていない場合、このヘッダーはプロキシによって追加されないため、「502 Bad Gateway」エラーは発生しません。これはSWGプロキシの問題ではありません（これはSWGプロキシの問題ではありません）。このエラーは、アップストリームWebサーバが標準のXFFヘッダーをサポートしないように誤設定されていることに起因します。

解決方法

この問題を解決するには、選択的な復号化リストを使用して、特定のドメインのHTTPSインスペクションをバイパスします。

- 517アップストリーム証明書の失効
- 証明書およびTLSプロトコルエラー
- 内部テスト用にSWG DCを手動で選択

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。