# Secure Web Gateway SWG Webサイトアクセスの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、クラウドベースプロキシ（セキュアWebゲートウェイ/SWG）経由でルーティングされ、Direct Internet Access(DIA)を使用していない場合に、Webサイトへのアクセスの問題を診断するための構造化された方法論について説明します。

- 範囲：Cisco Umbrella SIGとCisco Secure Accessの両方に適用されます。

### 前提条件と重要な警告

- 再現可能な問題に対してすべてのトラブルシューティングが実行されることを確認します。
- HAR（HTTPアーカイブ）ファイルと同時パケットキャプチャ(PCAP)を収集して、分析に必要な正確なデータを提供します。
- プロキシポリシーの変更（復号化やインスペクションのバイパスなど）は、セキュリティポスチャに影響を与える可能性があります。適用されるのはトラブルシューティングの場合か、推奨される場合のみです。

## プロキシレベルのエラーの特定

一般的なプロキシ干渉インジケータには、次のものがあります。

- 502不良ゲートウェイ
- 515アップストリーム証明書の信頼できない
- 517アップストリーム証明書の失効
- 403禁止
- 取り消された証明書
- 暗号スイートの不一致
- Webサイト接続のタイムアウト

# トラブルシューティング手法

## ステップ1：トラフィックがプロキシを通過することを確認する

- データ収集：問題が発生したときにHARファイルとPCAPを生成します。
- ヘッダー分析：HTTP応答のViaヘッダーを検査します。`s_proxy`（Nginxプロキシ）または`m_proxy`（モジュラプロキシサービス/MPS）が存在することで、トラフィックのプロキシ処理を確認できます。
- TCPストリーム：WiresharkでTCPストリームに従って、接続が宛先IPではなくプロキシのIPにあることを確認します。

## ステップ2:TLS復号化ステータスの確認

- ブラウザ検査：ブラウザのアドレスバーのロックアイコンをクリックします。Cisco Secure Accessルート証明書が証明書チェーンに含まれている場合、HTTPSインスペクションがアクティブになります。
- 検証：HAR/PCAPファイル内のViaヘッダーを相互参照します。
- OpenSSLコマンド：証明書チェーンを検査するには：
  `openssl s_client -connect www.example.com:443 -showcerts`
  このコマンドは、サーバによって提示される証明書チェーンをチェックします。直接検証のためにプロキシを通過するマシンから実行します。

## ステップ3：分離と排除のプロセス

1. フェーズA - HTTPSインスペクションのテスト（Nginxレイヤ）：
   - 問題のあるドメインをSWGの「Do Not Decrypt」リストに追加します。
   - ファイルインスペクションを有効のままにします。
   - 問題が解決した場合：根本的な原因はNginx SSL/TLSインスペクションである可能性があります。PCAPを分析して、暗号の不一致やSNIの問題がないかどうかを確認します。動作を比較するには、プロキシの有無にかかわらず`curl`を使用します。
   - 問題が解決しない場合：フェーズBに進みます。
2. フェーズB – テストファイルインスペクション（スキャンレイヤ）：
   - 特定のトラフィックのファイルインスペクションを無効にします。
   - 問題が解決した場合：根本的な原因はファイルスキャンエンジンにあります。PCAPとHARを確認し、ラボで再現して、特定のファイルまたはスキャンシグニチャが問題を引き起こすかどうかを確認します。
   - 解決しない場合：包括的なログと調査結果を添付の上、サポートに連絡してください。

# 一般的な問題とエラーコード

## 515アップストリーム証明書の信頼できない

このエラーは、SWGプロキシが宛先サーバの証明書を検証できないときに発生します。原因には、期限切れ、自己署名、または不完全な証明書チェーンが含まれます。

- HTTPSインスペクションON +ファイルインスペクションON: Webサイトは機能します。証明書エラーはありません。
- HTTPS Inspection ON + File Inspection OFF: 515エラーが表示され、ユーザレポートと一致する。
- HTTPSインスペクションOFF +ファイルインスペクションOFF (domain on Do Not Decrypt list):問題は確認されませんでした。

技術詳細：アップストリームサーバが中間証明書の欠落に対するAuthority Information Access(AIA)のフェッチに依存している場合、Nginxプロキシは失敗する可能性があります。これは、NginxがAIAをファイルスキャンプロキシサービスほど正常に処理しないためです。TLSハンドシェイク中のSNIおよびSANの不一致も障害をトリガーする可能性があります。

## 517アップストリーム証明書の失効

517エラーは、SWGプロキシのCRLまたはOCSPチェックで、アップストリームサーバの証明書が失効したことが検出されたことを意味します。

- トラブルシューティング：SSLラボやOpenSSLなどの外部ツールを使用して、失効ステータスを確認します。
- ドキュメンテーション:
  - Ciscoトラブルシューティングエラー517 – アップストリーム証明書の失効
  - 一般的な証明書およびプロトコルエラーについて

## 証明書エラー処理オプション

Cisco Secure Accessには、詳細なエラーバイパスを実現する新機能「証明書エラー処理オプション」が導入されており、復号化を完全に無効にする必要はありません。インスペクションによって証明書エラーを引き起こすドメインは、広範な「Do Not Decrypt」リストの代わりに、この機能を使用して管理できます。
この機能は、現在Umbrella SIGに存在します。CSAの機能要求の詳細

# 502不良ゲートウェイ

502エラーは、SWGプロキシが中継サーバとして動作しているときに、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示します。

– ダウンストリーム：クライアントからSWGプロキシ
– アップストリーム：宛先サーバへのSWGプロキシ

プロトコルエラー、TCPリセット、または不正なヘッダーが原因で、エラーは常にアップストリーム接続で発生します。

## 502の一般的な原因

- サポートされていないSWG暗号スイート
- クライアント証明書認証要求
- SWGプロキシによって追加されるヘッダー

## サポートされていない暗号スイート

原因：サーバーにはSWGでサポートされていない暗号が必要です（例：TLS_CHACHA20_POLY1305_SHA256）。
解決策：ドメインをSelective Decryptionリストに追加します。

テストコマンド：
プロキシを使用：

```
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
```

プロキシなし：

```
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
```

## クライアント証明書認証要求

原因：アップストリームサーバにはクライアント側の証明書が必要ですが、SWGはこの証明書をサポートしていません。
解決策：External Domains管理リスト(Umbrella SIG)またはBypass Secure Proxy(Cisco Secure Access)を使用して、プロキシからドメインをバイパスします。 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。

プロキシによって追加されたヘッダー

原因：一部のサーバーは、HTTPSインスペクションが有効な場合に、SWGによって追加されたX-Forwarded-For (XFF)ヘッダーで要求を拒否します。
解決策：HTTPSおよびファイルインスペクションの有無で動作を比較します。XFFが存在する場合にのみエラーが発生する場合、Webサーバの設定が誤っている可能性があります。

例：

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

ステータスコード：502

```
curl https://www.xyz.com -k -o /dev/null -w "ステータスコード： %{http_code}" -s
```

ステータスコード：200

位置情報のXFFヘッダーが追加されます。サーバが処理できない場合は、502エラーが発生します。

## 望ましくない可能性のあるPUAまたは破損したファイル

SWGがファイルインスペクションを使用してファイルをスキャンできない場合（たとえば、保護されたファイル、範囲要求されたファイル、破損したファイルなど）、ダウンロードがブロックされ、「Blocked - Potentially Unwanted Application (Protected File)」が報告されます

- トラブルシューティング：ブロックイベント中にHARをキャプチャします。一時的な回避策としてOverride Securityを使用します。ファイルが破損しているか悪意がある場合は、ソースで修正する必要があります。

潜在的に有害なカテゴリとレピュテーションブロック

- Talosを使用してWebレピュテーション(WBRS)を確認します。 ドメインが誤って分類されている場合は、COG JiraリクエストをTalosに送信して確認を求めてください。ターロスは安全または好ましいが、まだSWGブロックとして分類され、その後、我々はSWGのビーカーサービスからチェックする必要があります。

## SWG出力IPに対するAkamaiによるアクセス拒否

- SWGは共有出力IPを使用します。IPレピュテーションサービス（Brightcloudなど）によってこれらがブラックリストに登録されている場合、特定のサイトへのアクセスが拒否される可能性があります。

既知の問題：Youtubeのサインインボットとビデオが使用できません

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。