

セキュアアクセスにおけるSSL証明書およびハンドシェイクエラーについて

内容

問題

証明書およびTLSエラーが原因でブロックされたHTTPトラフィックをダッシュボードのアクティビティ検索で表示できるようになりました。この記事では、一般的なエラーメッセージのリストと、各エラーの簡単な説明を示します。

環境

- Cisco Secure Access:Secure Web Gateway SSLインスペクション

解決方法

アップストリーム証明書の期限切れ

Webサイトの証明書が有効期限を過ぎているため、Cisco Secure Accessはそれを信頼しません。これは修正するWebサイトの所有者にあるため、サイトのWebマスターに連絡して知らせてください。

アップストリーム証明書の自己署名

Webサイトは、信頼できる認証局によって発行された証明書ではなく、自身が署名した証明書を

提示しています。独立した機関が保証を行っていないため、Cisco Secure Accessでは証明書が本物であることを確認する方法がありません。

内部の少人数の対象者を対象としたリソースでは、自己署名証明書をよく目にしますが、ITセキュリティアプライアンスの管理者ポータルはその典型的な例です。Cisco Secure Accessは、自己署名証明書を信頼するように設定できないことに注意してください。

中間証明書がありません

Cisco Secure Accessでは、必要な中間証明書をすべて収集できなかったため、信頼の完全なチェーンを構築してルートに戻すことができません。

これが重要な理由です。Webサイトの証明書（「リーフ」）は中間証明書によって署名され、次に別の中間証明書によって署名され、信頼されたルートまで続きます。このチェーンをチェックアウトするには、Webサイトが自身の中間証明書と一緒に中間証明書を送信する必要があります。これらが欠落している場合、検証は失敗します。サイトのWebマスターに通知してください。

例外が1つあります。証明書に「Authority Information Access(AIA)」拡張子が含まれている場合、Cisco Secure Accessは欠落している中間証明書を自動的に取得しようとします。これは、HTTPS復号化とファイルインスペクションの両方がオンになっている場合にのみ機能することに注意してください。

アップストリーム証明書にサブジェクト名がありません

証明書には、サブジェクト名（識別名）またはサブジェクト代替名は含まれません。つまり、証明書が誰に属するかを明確に識別するものは何もありません。これがないと、Cisco Secure Accessでは検証できません。これは、Webサイトの所有者が修正する必要があるものです。

アップストリーム証明書に共通名がありません

証明書には共通名(CN)がありません。これは、従来サイトのホスト名を保持し、アクセスしているサイトに実際に証明書が属していることを確認するのに役立つフィールドです。最近では、このチェックは実際にサブジェクト代替名(SAN)に依存し、CNはレガシーフィールドと見なされていますが、CNが存在しないことがこのエラーを引き起こす可能性があります。アドレス指定を受けるためにWebマスターに連絡します。

信頼できないアップストリーム証明書

Cisco Secure Accessはこの証明書を信頼しません。通常、この証明書を発行したルートCAを認識しないためです。

Cisco Secure Access SWGには、信頼できるルート認証局のリストが組み込まれており、信頼できるプロバイダーから入手して最新の状態に保たれます。サイトの証明書がそのリストにないCAにトレースバックする場合、検証は失敗します。ルートCAが信頼できるCAであると確信できる場合は、テクニカルサポートに連絡して確認してください。

証明書のホスト名が予期したものと異なる

要求されたアドレスは証明書の名前と一致しません。共通名(CN)でもサブジェクト代替名(SAN)でもありません。アクセスしようとしているサイトに証明書が属していないように見えるため、Cisco Secure Accessではこの要求に対して証明書を信頼しません。ウェブマスターはこれを整理する必要があります。

アップストリーム証明書の失効

この証明書を発行した認証局(CA)はその証明書を無効にしました。つまり、この証明書は有効とは見なされなくなります。

Cisco Secure Accessでは、Online Certificate Status Protocol(OSCP)を使用してこれを確認します。OSCPは、証明書が失効しているかどうかをリアルタイムでチェックします。サイトのWebマスターに通知して、サイトを置き換えられるようにします。

TLSハンドシェイクエラー

サポートされていないアップストリーム暗号

Cisco Secure Access SWGが使用する暗号スイートがWebサイトでサポートされていないため、

TLSハンドシェイクを完了できませんでした。これは、より弱い暗号しか提供しない古いサーバや旧式のサーバで発生する傾向があります。修正はサーバ側で行われるため、Webマスターに渡します。

アップストリームTLSバージョンの不一致

Cisco Secure Access SWGがサポートするTLSバージョンがWebサイトで使用されていないため、ハンドシェイクが失敗しました。現在、Cisco Secure Access SWGプロキシはTLS 1.2およびTLS 1.3で動作します。クライアントから着信する接続と、宛先サーバへの接続の両方で動作します。

アップストリームDHキーが1024ビット未満

Webサイトで使用されているDiffie-Hellman(DH)キーがCisco Secure Accessで受け入れられるには弱すぎる(1024ビット未満)ため、ハンドシェイクを完了できませんでした。これはサーバ側の制限であるため、ウェブマスターはこれを強化する必要があります。

回避策

Cisco Secure Accessで設定を変更することで、これらの問題を回避できます。

この操作は、サーバーと証明書の信頼性が信頼できる場合にのみ実行する必要があります。

「選択的復号化リスト」エントリを使用して復号化を無効にする回避策と、「外部ドメイン」エントリを使用してCisco Secure Accessからのトラフィックを完全にバイパスする回避策があります。復号化が無効になっている場合、Cisco Secure Accessは証明書検証を実行しません。

ほとんどの場合、Cisco Secure Accessからトラフィックがバイパスされるときに、ブラウザは依然としてエラーまたは警告を表示します。Webブラウザは同様の証明書検証を実行します。

原因

Cisco Secure Access SSLインスペクションプロキシがTLSハンドシェイクを完了できませんでした。多くの場合、宛先でCSA再署名証明書を拒否する証明書ピンングが使用されていることが原因です。

- ・ 証明書のピンング：クライアントのハードコードに必要な証明書のフィンガープリント
- ・ CSA CA not trusted on endpoint: inspection CA cert not deployed to trusted root store (エンドポイントでCSAが信頼されていない：検査用CA証明書が信頼されたルートストアに展開されない)

関連コンテンツ

- ・ [シスコのテクニカルサポートとダウンロード](#)

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。