エラーのトラブルシューティング"517アップストリーム証明書の失効"

内容

はじめに

このドキュメントでは、HTTPS urlを参照する際のエラー「517 Upstream Certificate Revoked」のトラブルシューティング方法について説明します。

問題

Umbrella Secure Web Gateway(SWG)WebプロキシがHTTPSインスペクションを実行するように設定されている場合、ユーザは「517 Upstream Certificate Revoked」エラーページを受け取る場合があります。このエラーは、要求されたWebサイトがTLSネゴシエーションでデジタル証明書を送信し、その証明書の発行者または同様の機関によってステータスが「無効」になっていることを示します。失効した証明書は有効ではありません。

13351060307092

原因

UmbrellaクライアントがUmbrellaセキュアWebゲートウェイ経由でHTTPS要求を行うと、SWGはOnline Certificate Status Protocol(OCSP)を使用して証明書失効チェック(CRL)を実行します。 OCSPは、証明書の失効ステータスを提供します。SWGは、Umbrellaクライアントに代わって証明書失効ステータスのOCSP要求を行います。

SWGは、要求されたWebサーバの証明書および信頼できるルート証明書へのパス内のすべての発行中間証明書の証明書失効ステータスを判別します。これらのチェックにより、有効な信頼のチェーンが発行後に無効になっていないことが確認されます。

OCSP失効チェックを使用するデジタル証明書では、「Authority Information Access」X.509拡張に1つ以上の「OCSP」フィールドが含まれます。フィールドには、証明書の失効ステータスを照会できるOCSP「エンドポイント」（Webサーバ）のHTTP URLが含まれています。SWGは、次のいずれかを示す応答を受信するまで、証明書内の各OCSP URLに対して要求を行います。

- 証明書が有効である（失効していない）場合、SWGはWeb要求の続行を許可します。または、
- ocspの「certificate valid」応答以外の応答（たとえば、証明書が失効している、サーバが現時点で応答できない、HTTPエラーステータス、ネットワーク/トランスポート層タイムアウトなど）がある場合、SWGが適切なエラーページまたはメッセージを表示し、Web要求が失敗します

OCSP応答は通常キャッシュされ、将来のチェックへの応答に使用されることに注意してください。キャッシュ時間は、OCSP応答でサーバによって設定されます。

直接参照するときの動作が異なる

Webクライアントは、クライアントに応じて、さまざまな失効チェックメカニズムを使用できます。たとえば、GoogleのChromeブラウザはデフォルトでは OCSPまたは標準CRLメソッドを使用しません。その代わり、ChromeはCRLSetと呼ばれる独自バージョンのCRLを使用します。これは、Secure Web Gatewayでは使用されません。その結果、証明書の失効ステータスを確認する際に、ChromeはSWGと同じ結果を生成しない場合があります。

ただし、CRLSetのドキュメントに記載されているように、「場合によっては、Chromiumの動作に関係なく、基礎となるシステム証明書ライブラリが常にこれらのチェックを実行します」という点に注意してください。 したがって、ご使用のローカル環境に応じて、ブラウザまたはオペレーティングシステムの暗号化サービスライブラリ（SChannel、Secure Transport、NSSなど）のいずれかによって、OCSPおよび/またはCRLチェックを実行できます。

また、OCSPチェックとCRLチェックでは同じ結果が生成されるとは限りません。

ブラウザまたはオペレーティングシステムベンダーのマニュアルを参照して、ブラウズ時にクライアントが実行する証明書失効チェックを確認してください。

解決方法

有効な証明書の使用は、Webサーバ管理者の責任です。失効した証明書の修復は、サーバー管理者がサーバー上で実行する必要があります。Cisco Umbrellaはこのプロセスをサポートできません。

Cisco Umbrellaでは、無効になった証明書を使用するWebサイトへのアクセスを強くお勧めします。回避策は、サイトが失効した証明書を使用する理由をユーザが十分に理解し、リスクを完全に受け入れる場合にのみ使用できます。

このエラーを回避するには、サイトのドメイン名を含む選択的復号化リストを作成することで、サイトをHTTPSインスペクションから除外できます。サイトへのアクセスを許可するWebポリシーにSelective Decryption List(SPD)が適用されます。または、サイトを外部ドメインリストに追加して、SWGをバイパスし、トラフィックをサイトに直接送信することもできます。

追加情報

サーバの証明書が失効しているかどうかの確認を希望するお客様は、失効ステータスを確認するように設計されたサードパーティツールを使用できます。特に、Qualys SSLラボのSSLサーバテストツールでは、証明書の有効性情報に加えて、OCSPとCRLの両方のチェックが実行されます。このツールは、次のURLからオンラインで入手できます。

- https://www.ssllabs.com/ssltest/analyze.html

Cisco Umbrellaでサポートケースをオープンする前に、このツールを使用して、517 Upstream Certificate Revokedエラーを生成するサイトを確認することをお勧めします。

次も参照してください。https://support.umbrella.com/hc/en-us/articles/4406133198100-

Certificate-and-TLS-Protocol-Errors

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。