UmbrellaセキュアWebゲートウェイでの516エラー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セキュアWebゲートウェイで516エラーが増加した場合のトラブルシューティング方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Umbrella Secure Web Gateway(SWG)に基づくものです。

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。

概要

HTTPSインスペクションを使用してUmbrellaセキュアWebゲートウェイ(SWG)プロキシをブラウズしているユーザは、2023年10月後半から、より頻繁に「516 Upstream Certificate CN Mismatch」エラーページを受信する可能性があります。

516エラーページは、Webサイトの証明書が、クライアントがサイトへのアクセスに使用するドメイン名と一致しない場合に表示されます。

エラーページの増加は、HTTP（暗号化されていない）方式を使用するURLの要求に対するChromeブラウザの処理の変更によるものです。Chromeは、最初にHTTPS（暗号化）スキームを使用してリソースをロードしようとします。HTTPSインスペクションが設定されている場合、SWGはWebサイトの証明書を検査し、証明書が受け入れられない場合は、516などのエラーコードを示すWebページを返します。

この問題を回避するには、HTTPSインスペクションをバイパスするようにWebポリシーを設定します。設定しない場合は516エラーが発生します。

516エラーの背景

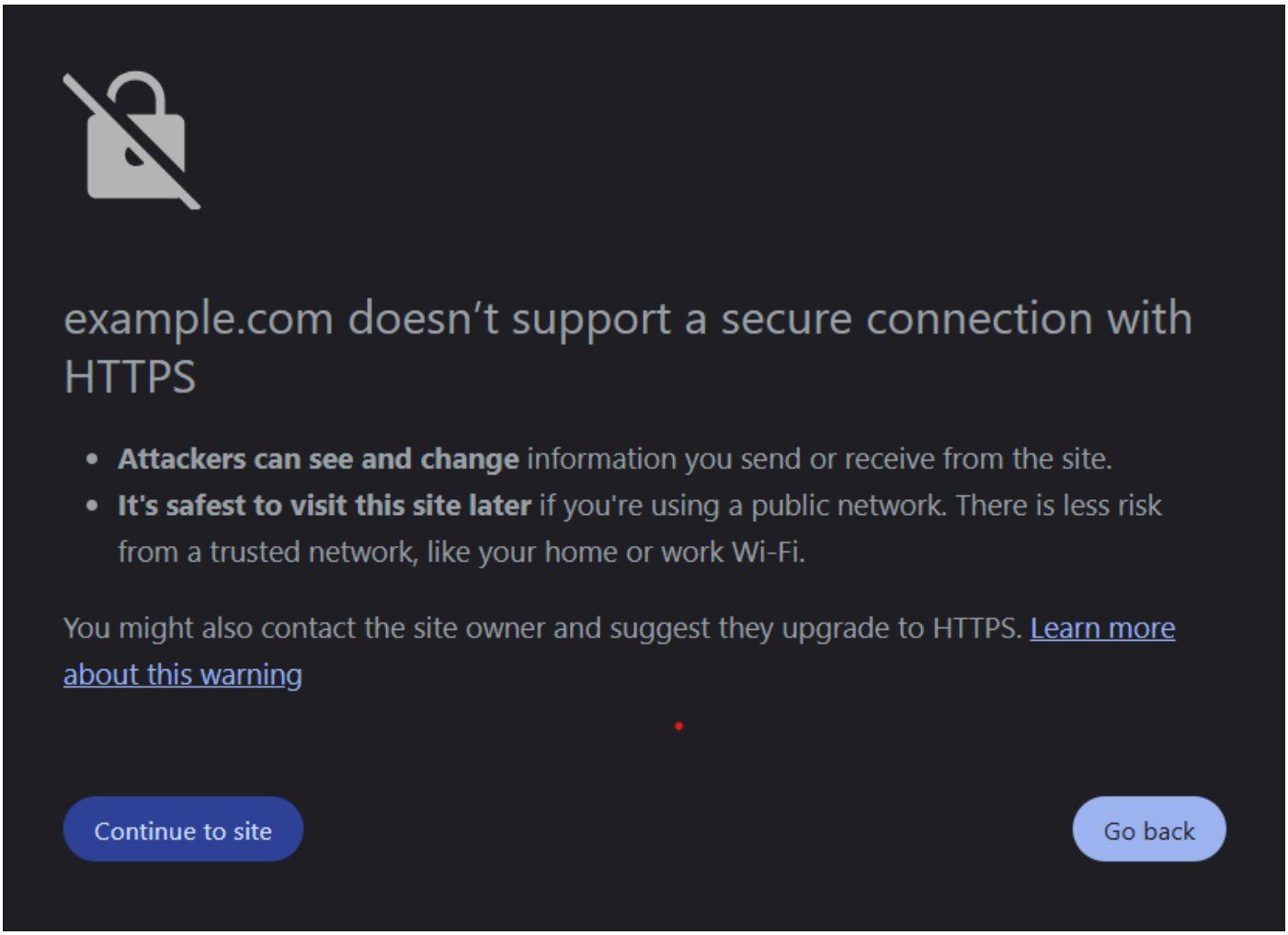
つまり、HTTPS経由でWebサイトにアクセスするために使用するドメイン名がサーバのデジタル証明書に含まれていない場合、Umbrella Secure Web Gatewayは516のエラーページを返します。Secure Web Gatewayが516エラーページを返す理由について詳しくは、Umbrella Knowledge Baseの記事「516 Upstream Certificate CN Mismatch」エラーを参照してください。

たとえば、http://www.example.com/path_to_contentという形式のHTTP URLのコンテンツを提供するサイトがあるとします。ユーザが同等のHTTPS URLを要求しても、サイトにSANがwww.example.comに一致する証明書がない場合(SANだけがexample.comに一致する場合など)、要求がSWGのHTTPSインスペクション機能を使用するWebポリシーによってUmbrellaのセキュアWebゲートウェイ(SGW)で処理されると、ユーザには516エラーが発生します。

Chromeの動作の変更

2023年10月後半に、GoogleはChromeブラウザの新機能のロールアウトを完了しました。その日を過ぎると、そのURLのHTTPSバージョンを使用して、HTTP URLの要求が自動的に行われます。たとえば、ユーザがhttp://www.example.comを要求すると、Chromeは最初にhttps://www.example.comを使用して要求に対応しようとします。

HTTPS URLの要求時にHTTPS関連のエラーを受信すると、ChromeはHTTP経由で同じコンテンツをロードしようとします。HTTP URLの要求が正常に実行されると、次の図に示すように、サイトがセキュアでないことを示すテキストと、続行するオプションをユーザに提供するリンクが表示された中間ページがChromeによって表示されます。



これは、Chromeの新機能のフォールバック動作です。

ただし、SWG経由でHTTPSインスペクションを使用してブラウズする場合、HTTPS 要求によってサイトから「ERR_CERT_COMMON_NAME_INVALID」などのHTTPS関連のエラーが生成されると、SWGによってエラーがインターセプトされ、516エラーページなどのSWGエラーページがChromeに返されます。このSWGコンテンツはChromeではHTTPS関連のエラーと見なされないため、フォールバック動作は発生せず、上の図のページではなく、SWGエラーページが表示されます。

新しいChromeの動作の詳細については、Chromiumブログと機能のGitHubリポジトリを参照してください。

エラーの原因の特定

ChromeがHTTP URLをHTTPS URLに自動的に昇格するようになったため、516エラーが生成されるWebサイトがユーザに頻繁に表示されるようになります。

Webサイトが原因で516応答などのHTTPS関連のエラーが発生していることを確認するには、Umbrellaを使用していないデスクトップシステムからChromeを使用してサイトを参照します。HTTPハイパーリンクをクリックする代わりに、URLのHTTPSバージョンをChromeのOmnibox（アドレスバーなど）に手動で明示的に入力してください。ハイパーリンクによってSWGで516エラーが生成された場合、SWGを使用せずにChromeでHTTPS URLを手動で要求すると、エラーメッセージ「ERR_CERT_COMMON_NAME_INVALID」が生成される場合があります

。 このエラーメッセージは、問題がWebサイトへのアクセスに使用されたドメイン名に対する誤った証明書であることを確認します。

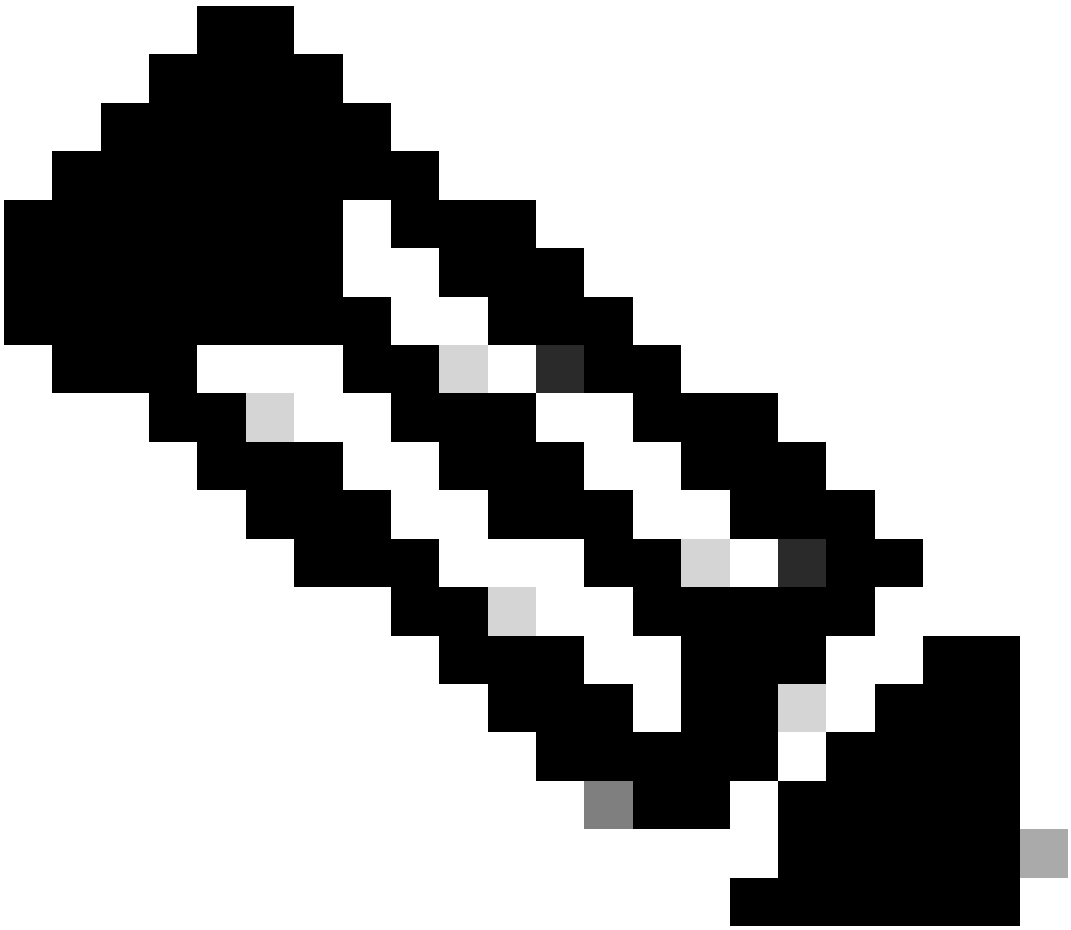
または、Qualys SSL Server Testサイトなどのオンラインツールを使用して、Webサイトの問題を診断します。

回避策

Umbrella管理者は、次のオプションのいずれかを使用してこの問題を回避できます。

1. これらのサイトに特化した宛先リストを作成し、HTTPSインスペクションを使用せずにWebポリシーに追加します。

2. 516のエラーページが生成されるサイトの選択的復号化リストを作成し、関連するすべてのWebポリシーにこの選択的復号化リストを追加します



注:HTTPリダイレクトや電子メールセキュリティシステムなどの要因により、サービスのHTTPS URLが元のHTTP URLに置き換えられ、必要なドメイン名が不明瞭になる場合があります。宛先リストまたは選択的復号化リストに対して正しいドメイン名を特定する

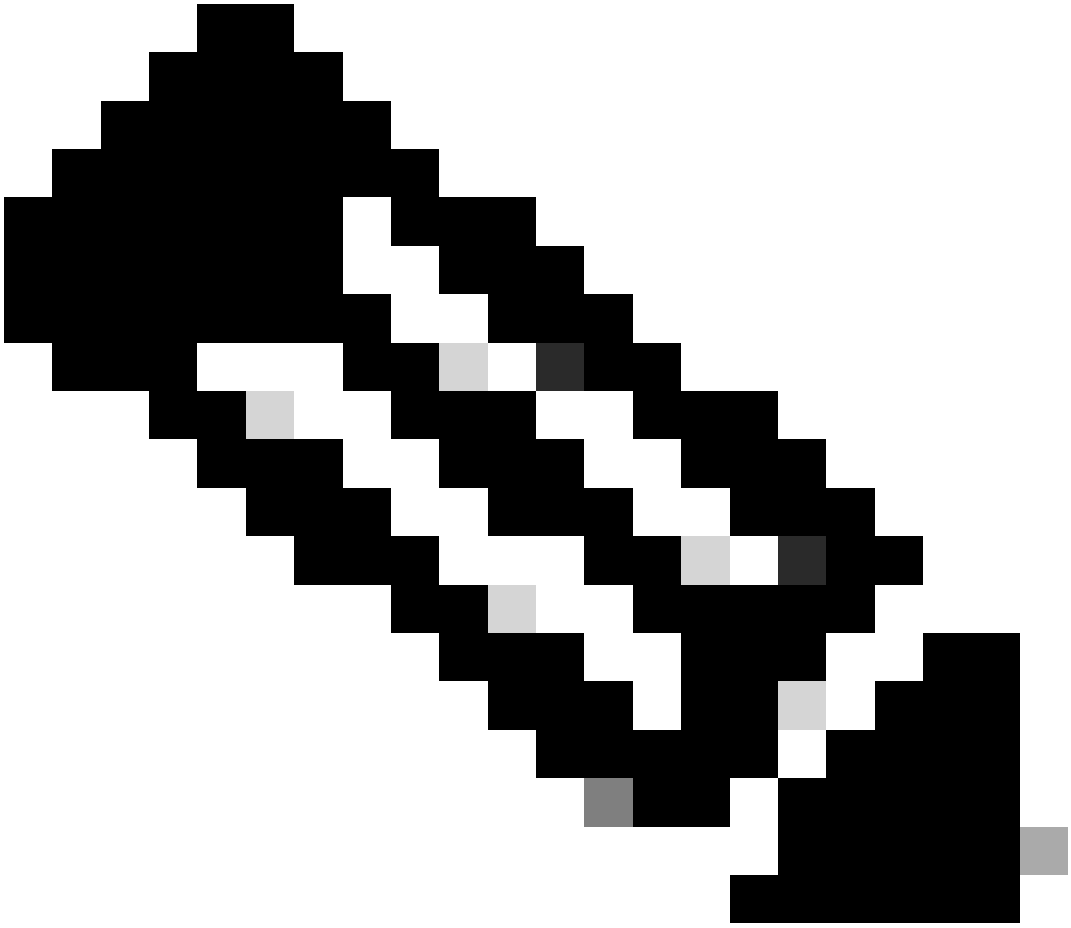
には、特定のツール（curl、Chrome Developer Tools、Eメールセキュリティベンダーのログなど）の使用を含む調査が必要な場合があります。

516エラーおよび電子メールシステム

HTML形式で電子メールを表示し、電子メール内のハイパーリンクを許可する電子メールシステムにより、エラーの頻度が516増加する可能性があります。電子メールを作成するときに、送信者がドメイン名を入力するか、電子メールの本文に貼り付けると、多くの電子メールシステムはプレーンテキストのドメイン名を自動的にハイパーリンクに昇格させます。通常、リンクが作成されると、スキームはHTTPSではなくHTTPになります。

たとえば、電子メールに文字列`example.com`を入力すると、ハイパーリンクwww.example.comとして表示されるHTMLコード`<a href="http://www.example.com">`を含む電子メールになる場合があります。

このような電子メールの受信者がそのHTTPハイパーリンクをクリックすると、クリックによってChromeが開いた場合、または電子メールの表示にChromeがすでに使用されている場合、リクエストは最初にHTTPSを使用します。



注：他のブラウザでもHTTPをHTTPSに昇格できます。

また、意図的にHTTP方式を使用する電子メール内のハイパーリンクも同様に処理されます。

一部の一般的なクラウドサービスは、サードパーティの取引電子メールサービスプロバイダーから、HTTPSハイパーリンクではなくHTTPハイパーリンクを使用して電子メールを送信します。Chromeが自動的にロードしようとしているHTTPSサイトは、この例のSeegridからのように、電子メールリンクのドメイン名に証明書エラーで応答できます。

これらの電子メールの受信者リストが大きい場合、SWGを介してクリック（または要求）が送信される多くのユーザは、516エラーなどのエラーを報告できます。電子メールサービスプロバイダーまたは電子メールを送信した組織に連絡して、証明書のエラーに対処してください。

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。