

セキュアアクセスにおけるSSL復号化証明書のエラー処理

内容

お問い合わせ内容

Cisco Secure AccessでSSL復号化が有効になっている場合、ユーザに証明書関連のエラーページが表示されます。証明書エラーの3つの特定のタイプに関して、複数の問い合わせを受けました。

- オリジンサーバ証明書の期限切れエラー
- 証明書にリストされている共通名またはサブジェクトの別名がアクセス先のドメインと一致しないという証明書のCN/SAN不一致エラー
- 接続問題を引き起こす元のサーバ証明書に組み込まれている証明書失効リスト(CRL)リンク

これらの証明書エラーは、通常Webブラウザに表示される警告に似ています。問題は、Cisco Secure Accessが証明書関連のエラーを処理できるかどうか、(ブラウザやコンテンツフィルタと同様に) 警告ページを表示した後で、警告が表示された後にアクセスを許可するか、すべての場合でアクセスを許可するかです。また、SSL復号化が無効になっている場合の動作、および証明書の問題に関係なくトラフィックが通過するかどうかを理解する必要があります。

環境

- Cisco Secure Access – インターネットアクセス (ローミングモジュール、VA、DNS、SWG、PAC、IPS、証明書)
- SSL暗号化解除機能が有効
- 証明書検証の問題が発生した複数のドメイン
- オリジンサーバで、有効期限やドメインの不一致など、さまざまな証明書の問題が発生する

解決策

証明書エラー処理の制限

証明書関連のエラー処理は、Cisco Secure Accessでは使用できません。この製品は以下をサポートしていません。

- 証明書の問題に関するブラウザのような警告ページの表示
- ドメイン固有の証明書エラー処理構成
- 宛先ドメインに基づくカスタムエラー処理
- コンテンツフィルタスタイルの警告ページとユーザ上書きオプション

SSL復号化の除外回避策

推奨されるアプローチは、セキュリティプロファイルの復号化設定を使用して、問題のあるドメインをSSL復号から除外することです。これは、次の方法で設定できます。

SSLインスペクションから特定のドメインを除外するには、Security Profile > Decryption Settingsセクションに移動します。

ドメインがSSL復号化から除外されると、次の動作が発生します。

- 除外ドメインのトラフィックはSSLインスペクションを完全にバイパス
- 証明書の検証はセキュアアクセスでは実行されません
- セキュアアクセスによって生成された証明書のエラーページが表示されない
- 証明書の問題が解決されない場合は、ユーザブラウザに元の証明書エラーが表示される可能性があります

SSL復号化が無効な動作

ドメインまたはグローバルでSSL復号化が無効になっている場合、Cisco Secure Accessは、証明書の問題に関係なく、トラフィックを通過（転送）させます。復号化が有効になっていないと、製品は証明書の検査や検証を行わず、すべてのHTTPSトラフィックが透過的に通過できるようになります。

原因

証明書エラーは、期限切れの証明書、CN/SANの不一致、CRLの接続性の問題など、発信元サーバでの正当な証明書検証の問題によって発生します。Cisco Secure Accessは、SSL復号化プロセスの一部として証明書の検証を実行します。この検証でエラーが発生すると、製品は潜在的に安全でない接続を防ぐためにエラーページを生成します。これは、SSLインスペクション機能の意図されたセキュリティ動作です。

関連コンテンツ

- [Cisco Secure Access Decryptionの設定に関するドキュメント](#)
- [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。