IPSおよびSWG復号化バイパスに対してSSEが復号化を行わない設定

内容

問題

財務カテゴリの宛先へのHTTPSトラフィックでは、財務カテゴリまたは特定のドメインをDo Not Decrypt(DND)リストに追加して、関連するアクセスルールを適用した後でも、発信元のWebサイト証明書ではなく、Cisco SSE証明書が引き続き提示されます。この動作は、ゼロトラストアクセスクライアント(TIA)経由でサイトにアクセスする際に見られ、特に、エンドツーエンドの証明書の可視性が必要なhttps://onlinesbi.sbi.bank.in/などの財務関連Webサイトへのアクセスに影響を与えます。

サイトまたはコンテンツカテゴリがDNDリストに追加されると、Cisco SSE証明書の代わりに元のWebサイトの証明書がブラウザに表示されることが期待される動作です。ただし、Cisco SSE証明書は引き続き提示され、DNDの設定にもかかわらずトラフィックの復号化が引き続き行われていることが示されています。

環境

- シスコセキュアサービスエッジ(SSE)
- ゼロトラストアクセスクライアント(TIA)接続
- グローバルIPS復号化が有効
- アクセスポリシーでIPSがアクティブ
- セキュリティプロファイル内の暗号化解除不可リストで構成された財務カテゴリ
- 対応するセキュリティプロファイルで適用されたアクセスルール

解決方法

この問題を解決するには、Cisco SSEが2種類の復号化を実行することを理解し、両方の復号化タ

イプに対して適切なDo Not Decrypt(DND)設定を行う必要があります。

SSE復号化タイプの理解

Cisco SSEは、次の2つの復号化プロセスを実行します。

- SWG(Secure Web Gateway)復号化:Webプロキシ復号化
- IPS復号化：侵入防御システム(IPS)復号化

Do Not Decryptセキュリティプロファイル内に設定されたエントリは、SWG復号化にのみ適用され、IPS復号化を阻止しません。グローバルIPS復号が有効で、いずれかのアクセスポリシーでIPSがアクティブになっている場合でも、IPS復号は行われ、結果としてCisco SSE証明書がブラウザに表示されます。

設定手順

ステップ1：提供された復号化しないリストにサイトまたはコンテンツカテゴリを追加します。

「System Provided Do Not Decrypt List」はすべてのIPSプロファイルに適用されます。このシステム提供リストにサイトまたはコンテンツカテゴリを追加すると、元のWebサイトの証明書が提示され、IPS復号化が効果的にバイパスされます。

手順2：追加のポリシー変更が必要ないことを確認します。

アクセスポリシー内でSystem Provided Do Not Decrypt Listを参照する必要はありません。リストは、すべてのIPSプロファイルに自動的に適用されます。

検証テスト

次の検証方法を使用して、適切な設定を確認できます。

方法1：提供されたシステムへのドメインの追加非復号化リスト

System Provided Do Not Decrypt Listに特定のドメインを追加すると、Cisco SSE証明書ではなく、元のWebサイトの証明書が提示される場合があります。

方法2：グローバルIPS復号化を一時的に無効にする（テスト用のみ）

グローバルIPS復号化を一時的に無効にすると、テストされたサイトの元の証明書も表示され、IPS復号化がCisco SSE証明書表示の原因であったことが確認されます。

予想される結果

適切に設定した後：

- 提供されたシステムに追加されたサイトまたはコンテンツカテゴリは、復号化しないリストに元のWebサイト証明書を提示します。
- 指定されたサイトまたはカテゴリでは、SWGとIPSの両方の復号化がバイパスされます。
- ブラウザには、Cisco SSE証明書ではなく、実際のWebサイト証明書が表示されます。

原因

この問題は、Cisco SSEがSWG復号化とIPS復号化という2つの異なる復号化プロセスを実行するために発生します。Do Not Decryptセキュリティプロファイル内で設定されたエントリは、SWG復号化をバイパスするだけです。グローバルIPS復号化が有効で、アクセスポリシーでIPSがアクティブな場合、IPS復号化は独立して実行され続け、サイトがセキュリティプロファイルのDNDリストに含まれていても、Cisco SSE証明書がブラウザに提示されます。

両方のタイプの復号化を完全にバイパスするには、サイトまたはコンテンツカテゴリをSystem Provided Do Not Decrypt Listに追加する必要があります。これは、すべてのIPSプロファイルに適用され、SWGとIPSの両方の復号化が行われないようにします。

関連コンテンツ

- セキュアなアクセスのための有効な非暗号化機能リストの作成

- セキュアアクセスの基本情報のトラブルシューティングと収集
- 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。