

ブラウザ以外のWebトラフィックに対するセキュアアクセスSSO認証動作

内容

お問い合わせ内容

IPSec接続を使用してCisco Secure Access(CSA)を実装する際に、セキュリティプロファイルでのSSO認証動作を明確にする必要がありました。具体的には、サイトがIPSecトンネル経由で接続されている場合に、どのタイプのアウトバウンドインターネットトラフィックがSSO認証をトリガーするかという問題が発生しました。

主な問題は、SSO認証がTCPポート80および443経由のブラウザベースのWebアクセスだけに適用されるのか、Webトラフィックを生成する非ブラウザベースのアプリケーションやデバイス（プリンタやWindows以外のエンドポイントなど）にも適用されるのかを理解することでした。接続されたサイトから発信されるさまざまなタイプのWebトラフィックに対して、認証プロンプトが表示され、アイデンティティプロバイダー(IdP)にリダイレクトされるタイミングに関する説明が必要でした。

環境

- Cisco Secure Access(CSA)の導入
- サイトとCSA間のIPSecトンネル接続
- SSO認証で設定されたセキュリティプロファイル
- プリンタやWindows以外のエンドポイントなど、さまざまなデバイスが混在する環境
- HTTPSインスペクションが有効
- SAML統合が設定されている

解決策

Cisco Secure AccessのSSO認証動作は、ブラウザベースのWebトラフィックのみを対象とするよう設計されています。システムは、Web要求がSSO認証の対象となる必要があるかどうかを判断するために、高度な検査プロセスを実行します。

SSO認証プロセス

Web要求をアイデンティティプロバイダー(IdP)にリダイレクトする前に、Cisco Secure AccessはHTTPSインスペクションを使用して、Cookieをサポートするブラウザから要求が発信されたかどうかを判断します。このインスペクションプロセスは、ブラウザベースのWebトラフィックとブラウザ以外のWebトラフィックを区別する重要なメカニズムです。

トラフィックの分類

ブラウザベースのトラフィック (SSO認証の対象)

- CookieをサポートするブラウザからのWeb要求
- ブラウザアプリケーションからのTCPポート80および443上のHTTP/HTTPSトラフィック
- HTTPSインスペクションCookie/ブラウザ検出を通過するトラフィック

ブラウザ以外のトラフィック (SSO認証の対象外)

- プリンタやその他のネットワークデバイスからのWebトラフィック
- Cookieをサポートしていないアプリケーション、またはブラウザとして識別されないアプリケーション
- ブラウザの検出に失敗するWebトラフィックを生成するWindows以外のエンドポイント
- HTTPSインスペクションブラウザの検証に合格しないWebトラフィック

SSO認証の前提条件

SSO認証が環境で正常に機能するためには、次の前提条件を満たす必要があります。

- 正常に動作するSAML設定が存在する必要があります。
- XFFを使用したプロキシネットワークまたはNATを使用しないトンネル (IPサロゲートには内部プライベートIPへの可視性が必要)
- HTTPSインスペクションを有効にする必要があります。
- ブラウザセッションはcookieを保持する必要があります (セッション終了時にcookieを削除するか、またはブラウズを装わないことはお勧めしません)。
- ロケーション間で重複しないIPアドレス、または重複が存在する場合は適切なサイト分離。

原因

この動作は、Cisco Secure Accessの設計上の動作です。SSO認証メカニズムは、Webブラウザを介したインタラクティブユーザセッションを対象とするように特別に設計されており、自動システムおよび非インタラクティブデバイスは、認証を中断することなくWebリソースにアクセスできます。この設計により、認証リダイレクトやCookieベースのセッションを処理できない自動プロセス、デバイス管理インターフェイス、およびアプリケーションの中断を防止できます。

関連コンテンツ

- [SAML統合の設定 – SAMLのIPサロゲートの有効化](#)
- [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。