SAML認証とPACベースのトラフィック転送を使用する共有コンピュータ環境向けのSecure Web Gateway(SWG)におけるユーザ単位の識別とポリシー適用の課題

内容

お問い合わせ内容

SAML認証とPACベースのセキュアアクセス、またはブランチからインターネットへのトラフィック転送を使用するCisco Secure Web Gateway(SWG)の導入では、共有コンピュータに最初にログインしたユーザだけがWebトラフィックおよびポリシー適用対象として正しく識別されます。 ユーザを切り替えると、IPサロゲートオプションが無効でPACファイルが使用されている場合でも、後続のWebトラフィックは最初のユーザに帰属し続けます。 DNSクエリはUmbrella仮想アプライアンス経由で正しいアクティブユーザを反映しますが、Webログとファイアウォールログはアクティビティを以前のユーザに永続的にマッピングします。 この要求は、共有コンピュータ環境でSWGがユーザごとの識別とポリシー適用をサポートするかどうかを判断し、正しいユーザマッピングを保証する方法を決定することです。

環境

- DNS解決のための仮想アプライアンス。
- ユーザアイデンティティのSAML認証
- トラフィック転送とPACファイルおよびPACファイルなしの混在。
- IPサロゲートオプションを有効にし、特定のサブネットとホストをクッキーのサロゲート用にバイパス。
- オンプレミスデバイス。リモートエンドポイントやユーザは不要。

解決策

この問題は、次の点を考慮したユーザ教育と設定ガイダンスによって解決されました。

- PACファイルでCookieサロゲート識別子を使用します。 トラフィックは、ネットワークトンネルに対してルーティングすることも、またはネットワークトンネルからルーティングすることもできます。
- PACファイルなしでCookie Surrogate IDを使用しますが、トラフィックはネットワークトンネル経由でルーティングする必要があります。
- クッキーサロゲートを適用するアクセスポリシーでは、セキュリティプロファイルでSAML認証を有効にする必要があります。

- Cookieサロゲートトラフィックは、ブラウザベースのトラフィック専用です。 ネットワークとして送信元IDを使用するマシンからの非クッキートラフィック（たとえば、TeamsまたはWebexトラフィック）を識別するには、別のルールが必要です。
- SWGモジュールは、cookieのサロゲートが機能するために使用できません。
- IPサロゲートも有効な場合は、Cookieサロゲートを使用するプライベートIPアドレス/サブネットをバイパスリスト（「ユーザーとグループ」–「構成管理」–「詳細設定」）に追加する必要があります。
- cookieサロゲートのバイパスリストも、より短いプレフィックスと一致します。 たとえば、
  10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
  加するとします。
- Cookieサロゲートは、複数のIDを保持するためにログアウトする必要なく、マシンからのユーザの切り替えをサポートします。

トラブルシューティングの多くは、ポリシーテストとアクティビティ検索です。

原因

共有コンピュータ環境でユーザを誤って識別する根本的な原因は、主にユーザの教育にあります。

関連コンテンツ

- 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。