セキュアなWebゲートウェイトラフィックにSAML IDが適用されない場合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、Secure Web Gateway(SGW)トラフィックに適用されないSAML IDのトラブルシューティング方法について説明します。

SAML IDはWebトラフィックに適用されません

SAML IDがどのWebトラフィックにも適用されない場合は、Umbrellaのドキュメントを参照して、セットアップが正しく完了していることを確認してください。次の設定項目を入力する必要があります。

- 「Deployments > SAML Configuration」で設定およびテストされたIdP設定
- Deployments > Web Users and Groupsでプロビジョニングされたユーザ/グループのリスト
- SAMLは、「Policies > Web Policies」の該当するポリシー*で有効にする必要があります。
- Policies > Web Policiesで、該当するポリシーのHTTPS復号化を有効にする必要があります

WebポリシーでのSAMLの有効化

SAMLおよびHTTPS復号化は、該当するネットワークまたはトンネルIDに適用されるポリシーで有効にする必要があります。これらの機能はユーザが特定される前に適用されるため、重要なポリシーは「接続方法」に適用されます。

SAMLポリシーは、次のように順序付けする必要があります。

1. より高い優先度：ポリシーがユーザ/グループに適用されます。このポリシーは、認証されたユーザーのコンテンツ/セキュリティ設定を決定します。
2. LOWER Priority：ポリシーはネットワーク/トンネルに適用されます。このポリシーでは

SAMLが有効になっており、初期認証がトリガーされます。

特定のWebトラフィックにSAML IDが適用されない

IPサロゲート（デフォルトの動作）

ユーザの識別の一貫性を向上させるため、新しいIPサロゲート機能を有効にすることをお勧めします。この機能は、すべての新規Umbrella SAMLカスタマーに対して自動的に有効になりますが、既存のUmbrellaカスタマーに対しては手動で有効にする必要があります。

IPサロゲートは、内部IP >ユーザ名情報のキャッシュを使用します。これは、SAML識別がすべてのタイプの要求に適用できることを意味します。Webブラウザ以外のトラフィック、Cookieをサポートしないトラフィック、およびSSL復号化の対象とならないトラフィックも対象となります。

IPサロゲートは、ユーザ識別の一貫性を大幅に向上させ、管理上の負担を軽減できます。

IPサロゲートには次の要件があることに注意してください。

- 内部IPの可視性は、Umbrellaネットワークトンネルまたはプロキシチェーン展開とX-Forwarded-Forヘッダーを使用して提供する必要があります。 これは、UmbrellaのホストPACファイルでは機能しません
- 共有IPアドレスのシナリオではIPサロゲートを使用できない（ターミナルサーバ、高速ユーザスイッチング）
- ブラウザでCookieを有効にする必要があります。 ただし、初期認証ステップではCookieが必要です。

Cookieサロゲート（IPサロゲートは無効）

IPサロゲートを無効にすると、ユーザIDはサポートされているWebブラウザからの要求にのみ適用され、WebブラウザはCookieをサポートする必要があります。 SWGでは、Cookie内のユーザのセッションを追跡するために、すべての要求に対してブラウザがCookieをサポートする必要があります。 残念ながらこれは、このモードでは、すべてのWeb要求がユーザに関連付けられるとは想定されていないことを意味します。

このような状況ではSAMLは適用されず、ネットワーク/トンネルIDに割り当てられたデフォルトポリシーが代わりに使用されます。

- Webブラウザ以外のトラフィック
- cookieが無効のWebブラウザまたはIE拡張セキュリティ設定
- Cookieをサポートしていないocsp/証明書失効チェック
- Cookieをサポートしない個々のWeb要求。 場合によっては、Webサイトのコンテンツセキュリティポリシーにより、個々の要求に対してCookieがブロックされることがあります。この制限は、一般的なコンテンツ配信ネットワークの多くに適用されます。
- SAMLバイパスリストを使用してターゲットドメイン/カテゴリがSAMLからバイパスされた場合
- Umbrella Selective Decryption リストを使用してHTTPS復号化からターゲットドメイン/カ

テゴリがバイパスされた場合。

これらの制限があるため、関連するネットワーク/トンネルポリシーで適切な最小レベルのアクセスを設定することが重要です。デフォルトポリシーでは、ビジネスクリティカルなアプリケーション、ドメイン、カテゴリ、およびコンテンツ配信ネットワークを許可する必要があります。

または、IP Surrogatesシステムを使用して互換性を向上させることもできます。

SAMLバイパス

まれに例外が必要になります。 これは、SWGがSAML認証の要求を送信する際に、アプリケーションまたはWebサイトでサポートできない場合に必要です。 これは、次の場合に発生します。

- 非ブラウザアプリケーションでは、Webブラウザに似たユーザエージェントが使用されます
- スクリプトでは、Cookieテストで実行されたHTTPリダイレクトを処理できません
- ブラウジングセッションの最初の要求は、SAMLに正しくリダイレクトできないPOST要求（シングルサインオンURLなど）です

SAMLバイパスリストは、セキュリティを維持しながら認証からドメインを除外する（ファイルインスペクション）ための最適な方法です。

- 接続に使用するネットワーク/トンネルに影響を与える正しいポリシーに、SAMLバイパスリスト例外を適用する必要があります
- SAMLバイパスリストでは、トラフィックを自動的に許可しません。 ドメインは、関連するポリシーのカテゴリまたは宛先リストで引き続き許可されている必要があります。

SAMLバイパス：考慮事項

よく使用されるサイトや「ホームページ」の除外を追加する際は、SAMLへの影響を考慮することが重要です。SAMLは、ブラウジングセッションの最初の要求がHTMLページへのGET要求である場合に最も効果的です。 例：http://www.myhomepage.tld この要求はSAML認証のためにリダイレクトされ、後続の要求はIPサロゲートまたはCookieを使用して同じIDを想定します。

SAMLからホームページをバイパスすると、SAMLシステムで最初に確認される要求がバックグラウンドコンテンツ用であるという問題が発生する可能性があります。たとえば、http://homepage-content.tld/script.js にアクセスします。ブラウザが埋め込みコンテンツ（JSファイルなど）を読み込んでいるとき、SAMLログインページにリダイレクトするSAMLは不可能であるため、これは問題です。 つまり、ユーザが別のサイトに移動してログオンを開始するまで、ページが正しく表示されないか、正しく動作しません。

人気の高いサイトやホームページを検討する際は、次の選択肢を検討してください。

- 必要な場合を除き、ホームページや人気の高いサイトをSAMLまたはHTTPS復号化から除外しないでください
- ホームページを除外する場合、SAMLの非互換性を回避するために、そのサイトで使用されるすべてのドメイン（バックグラウンドコンテンツを含む）を除外する必要があります

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。