SWAでGoogleコンシューマアカウントのアクセスをブロックする

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)でGoogle WorkspaceまたはGoogle Consumer Accountsのアクセスをブロックするプロセスについて説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- SWAのグラフィックユーザインターフェイス(GUI)へのアクセス
- SWAへの管理アクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

<table>
<tr>
<td>ステップ1:Googleサイト用のカスタムURLカテゴリを作成します。</td>
<td>
ステップ 1.1： GUIで、Web Security Managerに移動し、CustomおよびExternal URL Categoriesを選択します。

ステップ 1.2： Add Categoryをクリックして、新しいカスタムURLカテゴリを作成します。

ステップ 1.3： 新しいカテゴリの名前を入力します。

ステップ 1.4： サイトセクションで次のURLを定義します。

<code>.google.com</code>

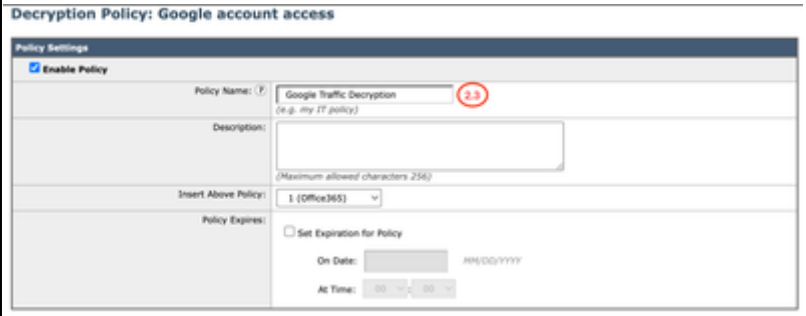
ステップ 1.5： 変更を送信します。

イメージ – カスタムURLカテゴリ

ヒント：カスタムURLカテゴリの設定方法の詳細については、「Secure Web Applianceでのカスタム URLカテゴリの設定」を参照してください。
</td>
</tr>
<tr>
<td>ステップ2：トラフィックを復号化します。</td>
<td>ステップ 2.1： GUIから、Web Security Managerに移動し、decryption Policiesを選択します。</td>
</tr>
</table>

ステップ 2.2： Add Policyをクリックします。

ステップ 2.3： 新しいポリシーのNameを入力します。



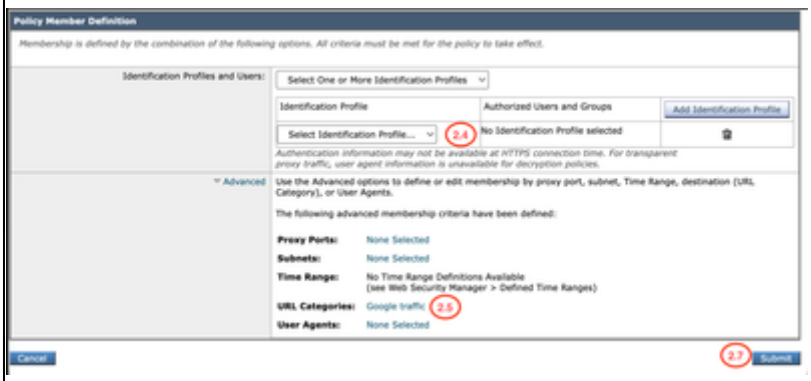
ステップ 2.4： このポリシーを適用するIDプロファイルを選択します。

ヒント:Microsoft URLの認証をバイパスし、このポリシーをすべてのユーザに設定する場合は、All Identification Profiles > All Usersの順に選択します。

ステップ 2.5： Policy Member Definitionセクションで、URL Categorieslinksをクリックしてカスタムカテゴリを追加します。

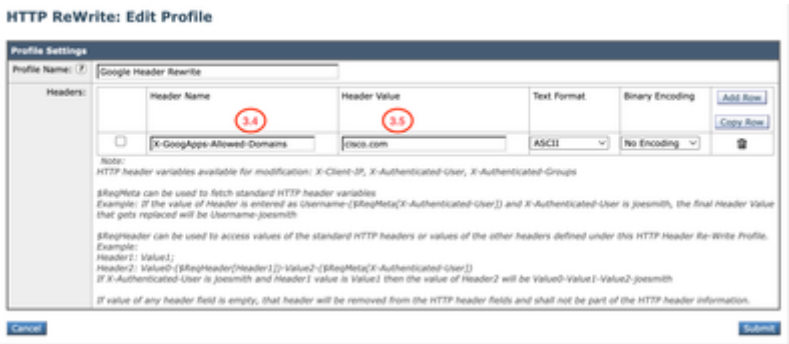
ステップ2.6：ステップ1で作成したURL カテゴリを選択します。

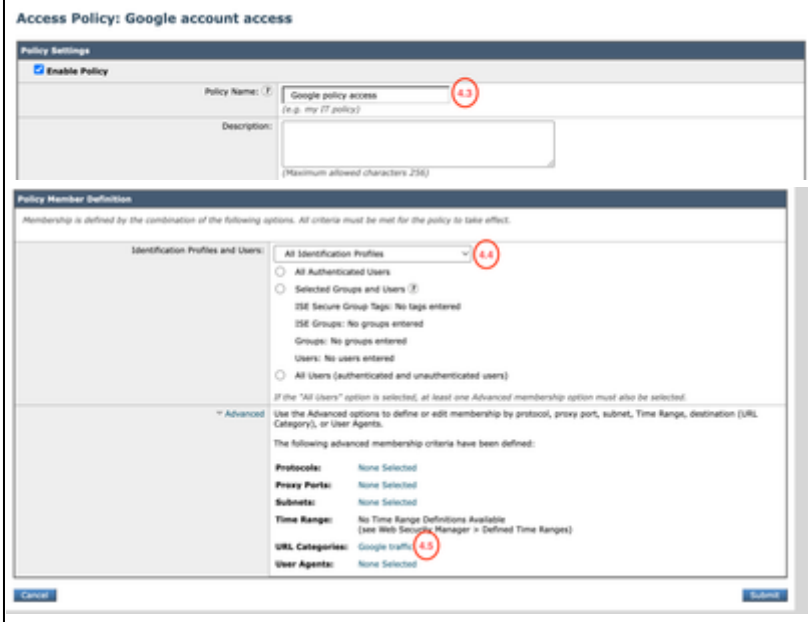
ステップ2.7:ClickSubmitをクリックします。

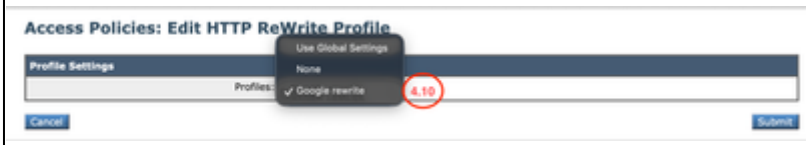


イメージ：復号化ポリシーの設定

ステップ 2.8： InDecryption Policiesページで、新しいポリシーのfromURL Filteringリンクをクリックします。

	図 – URLフィルタリング操作の編集 ステップ 2.9： カスタムURLカテゴリのアクションとしてDecryptを選択します。 ステップ2.10:ClickSubmitをクリックします。  図 – カスタムURLカテゴリの復号化
ステップ3:HTTPリライトプロファイルを作成します。	ステップ3.1:GUIから、Web Security Managerに移動し、HTTP ReWrite Profilesを選択します。 ステップ 3.2： 「プロファイルを追加」をクリックします。 ステップ 3.3： 新しいプロファイルのNameを入力します。 ステップ 3.4： firstHeader NameにはX-GoogApps-Allowed-Domainsを使用します。 ステップ 3.5： Restrict-Access-To-Tenantssettingでは、permitted tenant listのドメイン値を使用します。これは、ユーザがアクセスを許可されているテナントのカンマ区切りのリストである必要があります。 ステップ3.9:Submitをクリックします。  図 – HTTP書き換えプロファイルの追加

ステップ4：アクセスポリシーを作成します。	ステップ 4.1： GUIから、Web Security Managerに移動し、Access Policiesを選択します。 ステップ 4.2： Add Policyをクリックします。 ステップ 4.3： 新しいポリシーのNameを入力します。 ステップ4.4:（オプション）このポリシーを適用する必要があるIDプロファイルを選択します。 ステップ4.5:FromPolicy Member Definitionセクションで、URL Categorieslinksをクリックして、カスタムURLカテゴリを追加します。 ステップ4.6:ステップ1で作成したURL カテゴリを選択します。 ステップ 4.7： Submitをクリックします。  イメージ：アクセスポリシーの作成 ステップ4.8:InAccess Policiesページで、URL Filteringのアクションが Monitorに設定されていることを確認します。 ステップ4.9:HTTP ReWrite Profileのリンクをクリックして、このポリシーにHTTPヘッダープロファイルを追加します。  イメージ：アクセスポリシーのプロパティ

	ステップ 4.10： ステップ[3]で作成したHTTP ReWrite Profilesを選択します。  図 – HTTP書き換えプロファイルの追加 ステップ 4.11： Submitをクリックします。 ステップ 4.12： CommitChangesを実行します。

レポートとログ

ログ

カスタムフィールドをアクセスログまたはW3Cログに追加して、HTTPヘッダー書き換えプロファイル名を表示できます。

アクセスログの形式指定子	W3Cログのログフィールド	説明
%]	x-http-rewrite-profile-name（プロファイル名の書き換え）	HTTPヘッダー書き換えプロファイル名

アクセスポリシー名ごとにトラフィックのレポートを表示するWebトラッキングレポートを生成できます。

レポートを生成するには、次の手順を実行します。

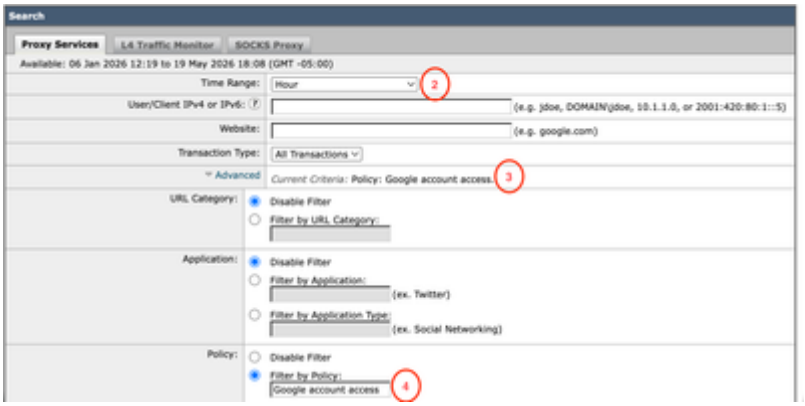
ステップ 1： GUIで、Reportingを選択し、Web Trackingを選択します。

ステップ 2目的の時間範囲を選択します。

ステップ 3 高度な条件を使用してトランザクションを検索するには、「詳細」リンクをクリックします。

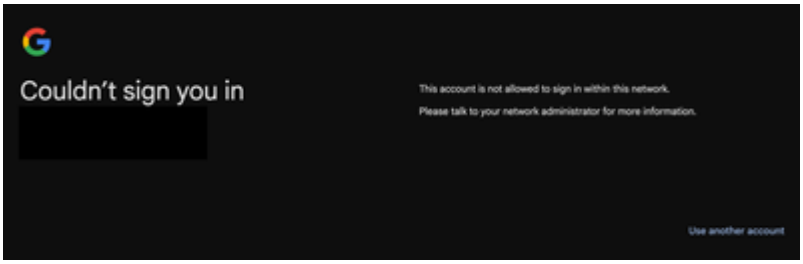
ステップ 4 Policyセクションで、Filter by Policyを選択し、前に作成したアクセスポリシーの名前を入力します。

ステップ 5 Searchをクリックして、レポートを確認します。



確認

Googleドメイン制限の設定が完了すると、ユーザはステップ3のヘッダー書き換えプロファイルで設定されたドメインの下にあるアカウントにのみアクセスできます。ユーザが別のドメインまたは別の個人Googleアカウントのアカウントにアクセスしようとした場合、アクセスは次の通知によって制限されます。



関連情報

WSAでのカスタムURLカテゴリの定義

AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド

Secure Web Applianceでの復号化証明書の設定

WSA HTTPヘッダーリライト

コンシューマアカウントへのアクセスをブロックする（Googleドキュメント）

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。