SWAでのMicrosoft O365テナント制限の設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

設定手順

レポートとログ

- ログ
- レポート

関連情報

はじめに

このドキュメントでは、Secure Web Appliance(SWA)でMicrosoft O365テナント制限を設定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あることが推奨されます。

- 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ました。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。

設定手順

ステップ 1：Webサイトのカスタムカテゴリを作成し	ステップ 1.1：GUIで、Web Security Managerに移動し、Custom and External URL Categoriesを選択します。

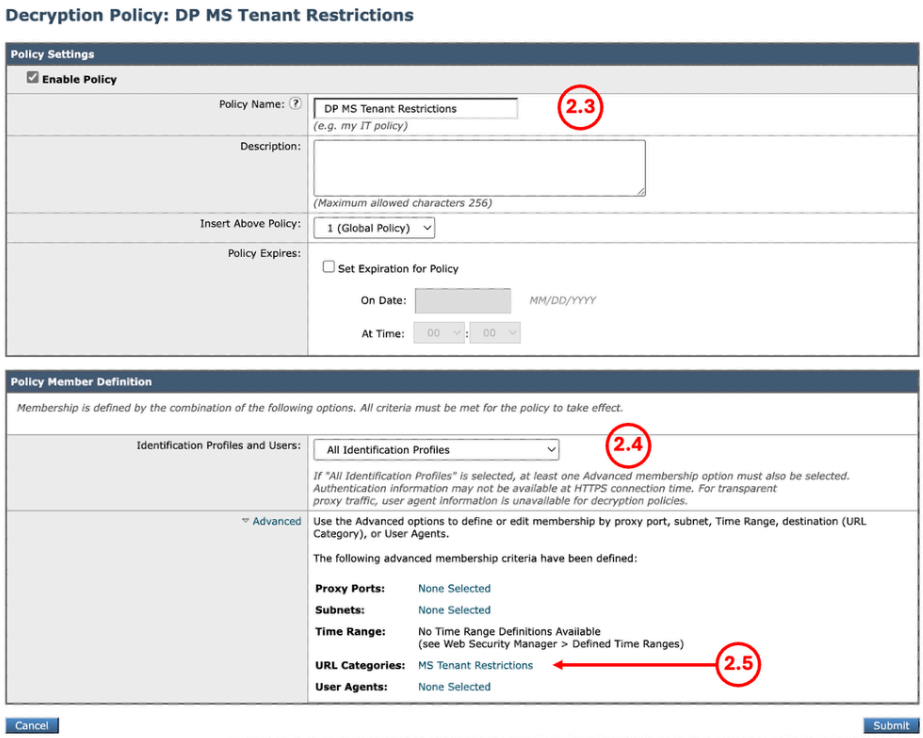
ます。	ステップ 1.2：Add Categoryをクリックして、新しいカスタムURLカテゴリを作成します。 ステップ 1.3：新しいカテゴリの名前を入力します。 ステップ 1.4：Sitesセクションで次のURLを定義します。 `login.microsoft.com, login.microsoftonline.com, login.windows.net` ステップ1.5：変更を送信します。 **Custom and External URL Categories: Edit Category** **Edit Custom and External URL Category** Category Name: MS Tenant Restrictions (1.3) Comments: List Order: 1 Category Type: Local Custom Category Sites: login.microsoft.com, login.microsoftonline.com, login.windows.net (1.4) Sort URLs *Click the Sort URLs button to sort all site URLs in Alpha-numerical order.* *(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)* Advanced — Regular Expressions: *Enter one regular expression per line. Maximum allowed characters 2048.* Cancel Submit 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、次のサイトを参照してください。https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
ステップ 2：トラフィックを復号化します。	ステップ 2.1： GUIで、Web Security Managerに移動し、Decryption Policiesを選択します ステップ 2.2：Add Policyをクリックします。 ステップ 2.3：新しいポリシーの名前を入力します。 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 Categoriesリンクをクリックして、カスタムURLカテゴリを追加します。

ステップ 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：[Submit] 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：Decryption Policiesページで、新しいポリシーに対するURL Filteringからのリンクをクリックします。

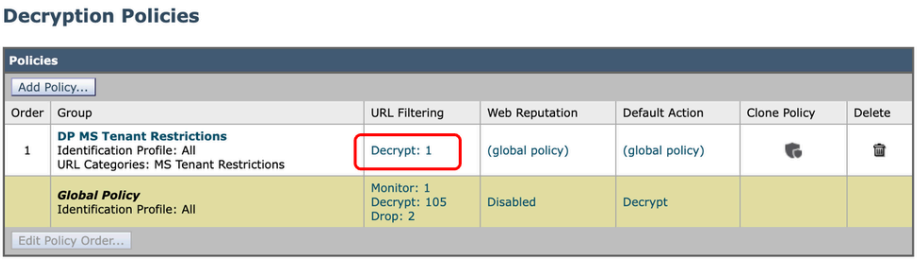


図 – URLフィルタリング操作の編集

ステップ 2.9：カスタムURLカテゴリのアクションとして復号化を選択します。

ステップ 2.10：[Submit] をクリックします。

<table>
<tr>
<td></td>
<td>
Decryption Policies: URL Filtering: DP MS Tenant Restrictions
Custom and External URL Category Filtering
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.
<table>
<tr><th rowspan="2">Category</th><th rowspan="2">Category Type</th><th rowspan="2">Use Global Settings</th><th colspan="6">Override Global Settings</th></tr>
<tr><th>Pass Through</th><th>Monitor</th><th>Decrypt</th><th>Drop</th><th>Quota-Based</th><th>Time-Based</th></tr>
<tr><td></td><td></td><td>Select all</td><td>Select all</td><td>Select all</td><td>Select all</td><td>Select all</td><td>(Unavailable)</td><td>(Unavailable)</td></tr>
<tr><td>MS Tenant Restrictions</td><td>Custom (Local)</td><td>–</td><td></td><td></td><td>✓</td><td></td><td>–</td><td>–</td></tr>
</table>
Cancel Submit
図 – カスタムURLカテゴリの復号化
</td>
</tr>
<tr>
<td>ステップ 3：HTTPリライトプロファイルを作成します。</td>
<td>
ステップ 3.1：GUIで、Web Security Managerに移動し、HTTP ReWrite Profilesを選択します。

ステップ 3.2：Add Profileをクリックします。

ステップ 3.3：新しいプロファイルの名前を入力します。

ステップ 3.4： 最初のヘッダー名には、Restrict-Access-To-Tenantsを使用します。

ステップ 3.5： Restrict-Access-To-Tenants設定には、<permitted tenant list>の値を使用します。この値は、ユーザにアクセスを許可す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 3.6：Add Rowをクリックします。

ステップ 3.7： 2番目のヘッダー名としてRestrict-Access-Contextを使用します。

ステップ 3.8：Restrict-Access-Context設定の場合、単一のディレクトリIDの値を使用して、テナント制限を定義するテナントを指定します。

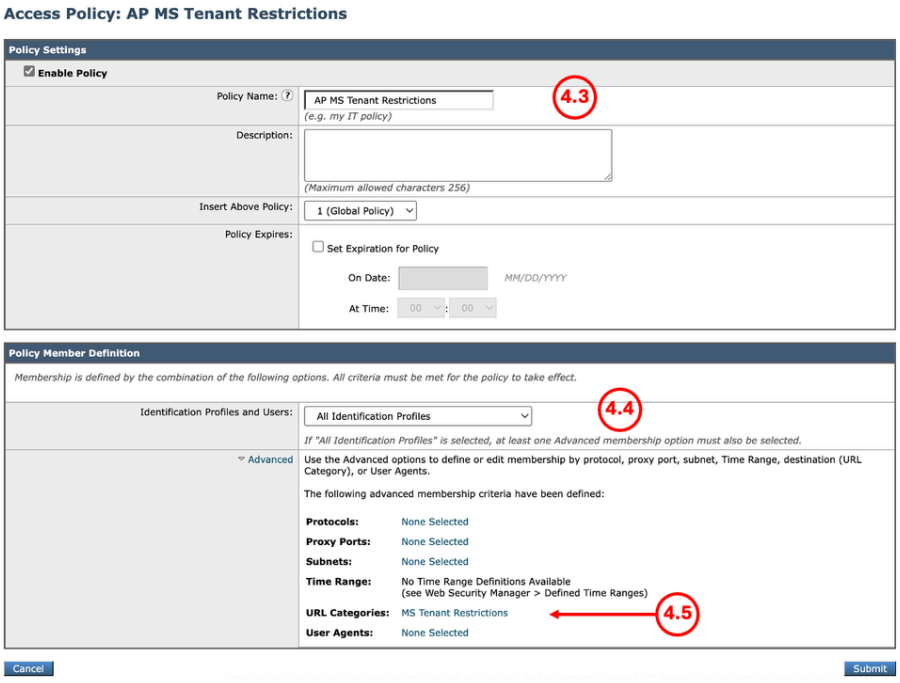
ステップ 3.9：[Submit] をクリックします。

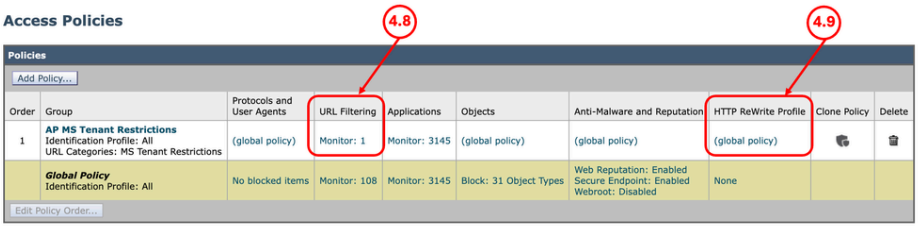
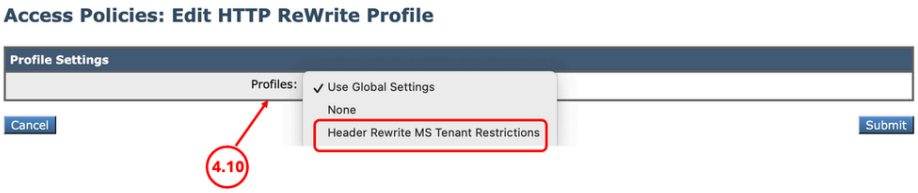
HTTP ReWrite: Edit Profile
Profile Settings
Profile Name: Header Rewrite MS Tenant Restrictions
Headers:
<table>
<tr><th></th><th>Header Name</th><th>Header Value</th><th>Text Format</th><th>Binary Encoding</th><th>Add Row
Copy Row</th></tr>
<tr><td></td><td>Restrict-Access-To-Tenants</td><td>[redacted]9.onmicrosoft.com</td><td>ASCII</td><td>No Encoding</td><td></td></tr>
<tr><td></td><td>Restrict-Access-Context</td><td>[redacted]2-9505-4097-a69a-c1553ef</td><td>ASCII</td><td>No Encoding</td><td></td></tr>
</table>
Note:
HTTP header variables available for modification: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups

$ReqMeta can be used to fetch standard HTTP header variables
Example: If the value of Header is entered as Username-{$ReqMeta[X-Authenticated-User]} and X-Authenticated-User is joesmith, the final Header Value that gets replaced will be Username-joesmith

$ReqHeader can be used to access values of the standard HTTP headers or values of the other headers defined under this HTTP Header Re-Write Profile.
Example:
Header1: Value1;
Header2: Value0-{$ReqHeader[Header1]}-Value2-{$ReqMeta[X-Authenticated-User]}
If X-Authenticated-User is joesmith and Header1 value is Value1 then the value of Header2 will be Value0-Value1-Value2-joesmith

If value of any header field is empty, that header will be removed from the HTTP header fields and shall not be part of the HTTP header information.
Cancel Submit
図 – HTTP書き換えプロファイルの追加
</td>
</tr>
</table>

	ヒント：テナント制限の詳細およびテナント情報の収集方法については、次のサイトを参照してください。Microsoft Learn - Restrict access to a tenant
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で、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：新しいポリシーの名前を入力します。 ステップ 4.4： 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 4.5：Policy Member Definitionセクションで、URL Categoriesリンクをクリックして、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：アクセスポリシーページで、URLフィルタリング

	のアクションがモニタ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：変更を確定します。

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

レポート

Webトラッキングレポートを生成して、AccessPolicy名でトラフィックのレポートを表示できます。

レポートを生成するには、次の手順を実行します。

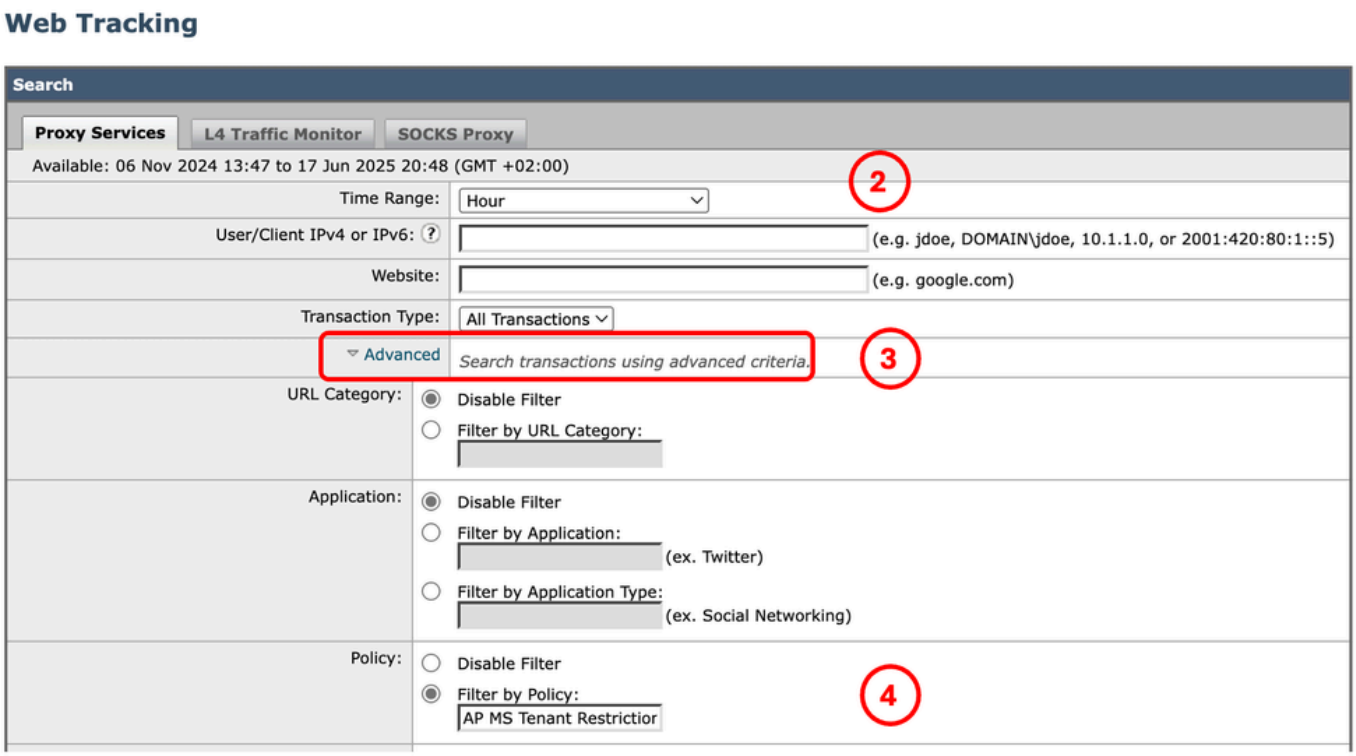
ステップ 1：GUIで、Reporting を選択し、Web Trackingを選択します。

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。



画像 – Webトラッキングレポート

関連情報

- AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド
- Cisco Secure Email & Web仮想アプライアンスインストールガイド
- Secure Web ApplianceでのカスタムURLカテゴリの設定：シスコ
- セキュアなWebアプライアンスのベストプラクティスの使用
- セキュアWebアプライアンス用のファイアウォールの設定
- Secure Web Applianceでの復号化証明書の設定
- SWAでのSNMPの設定およびトラブルシューティング
- Microsoftサーバを使用したSecure Web ApplianceでのSCPプッシュログの設定
- SWAで特定のYouTubeチャンネル/ビデオを有効にし、残りのYouTubeをブロックする

- Secure Web ApplianceのHTTPSアクセスログ形式について
- セキュアなWebアプライアンスのログへのアクセス
- Secure Web Applianceでの認証のバイパス
- Secure Web Applianceでのトラフィックのブロック
- Secure Web ApplianceでのMicrosoft Updatesトラフィックのバイパス

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。