SWAでの実行可能ファイルのダウンロードのブロック

内容

はじめに

このドキュメントでは、実行可能ファイルのダウンロードをブロックするようにSecure Web Appliance(SWA)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。

はじめる前に

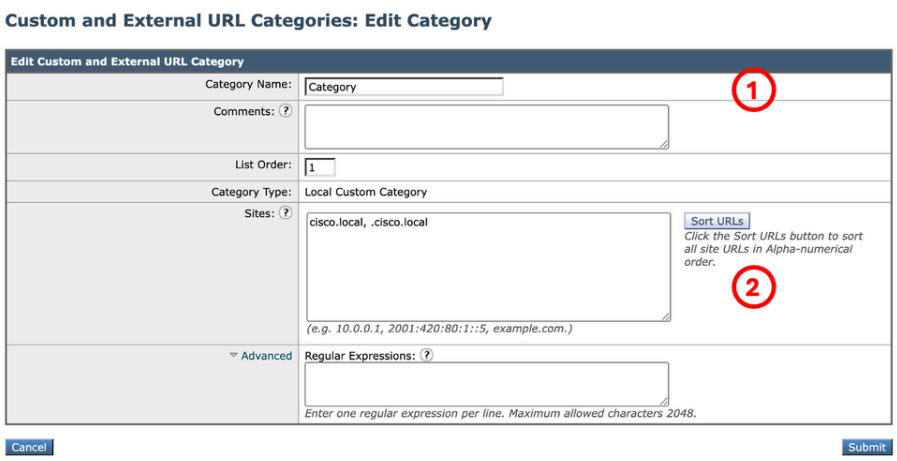
Cisco SWAは、Webコンテンツの(Multipurpose Internet Mail Extensions)MIMEタイプを検査することで、実行可能ファイルのダウンロードを効果的にブロックできます。SWAは、application/x-

msdownload、application/x-msi、およびその他の関連するMIMEタイプなどのファイルタイプを特定することで、実行可能ファイルがユーザに配信されるのを防ぐポリシーを適用します。MIMEタイプの検出に加えて、SWAはファイル拡張子フィルタリング、レピュテーションベースの分析、およびカスタムポリシールールを活用して、不要なダウンロードやリスクのあるダウンロードに対する保護をさらに強化できます。これらの機能により、組織はセキュアなブラウジング環境を維持し、マルウェア感染のリスクを軽減できます。

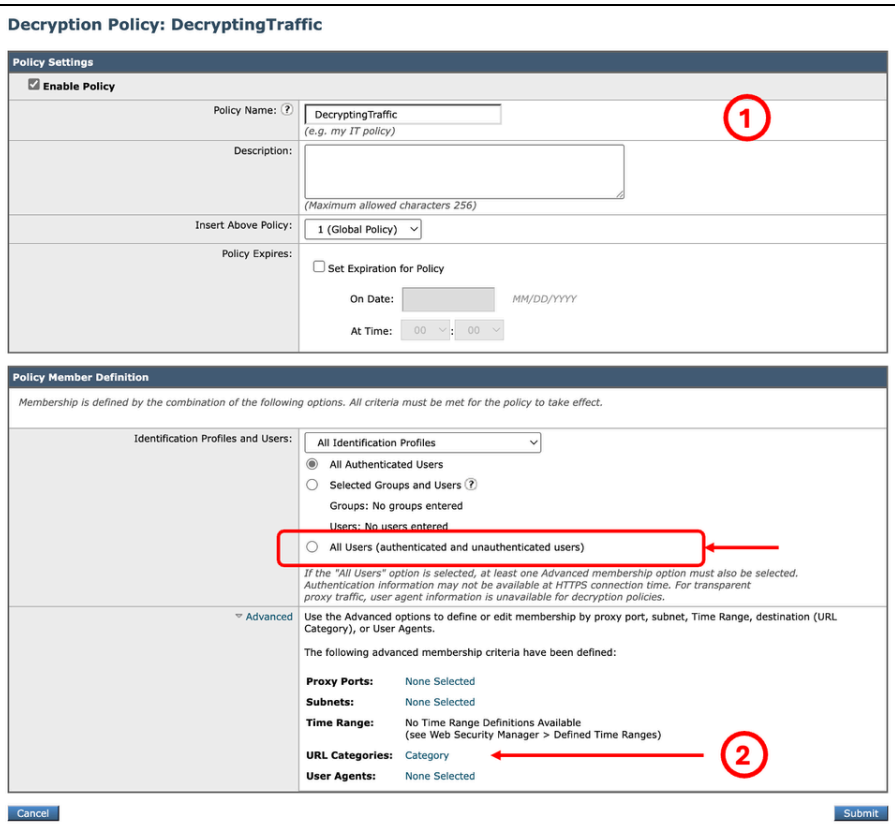
ヒント:SWAは、トラフィックが復号されない限り、ファイルのMIMEタイプを特定できません。

application/octet-streamは、ファイルにバイナリデータが含まれていることを示すために使用される汎用MIMEタイプです。ファイルの性質を指定しないため、より特定のMIMEタイプに適合しない任意のファイルに使用できます。このタイプは、通常、実行可能ファイル、インストーラ、および他の非テキストファイルに割り当てられます。これは、Webサーバが正確なタイプを判別できない場合に使用されます。

設定手順

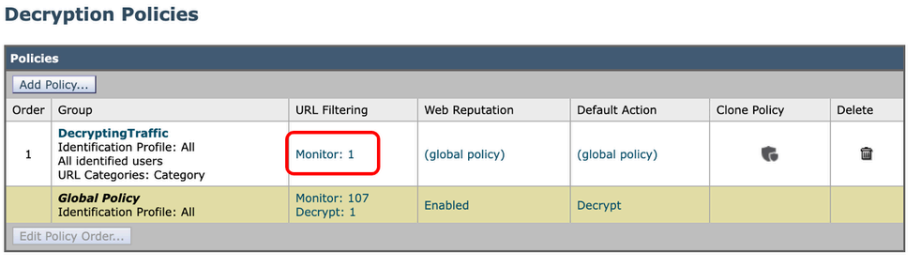
ステップ1:Webサイトのカスタムカテゴリを作成します。	ステップ1.1.GUIからWeb Security Managerに移動し、Custom and External URL Categoriesを選択します。 ステップ1.2：カテゴリの追加をクリックして、新しいカスタムURLカテゴリを作成します。 ステップ1.3:新しいカテゴリの名前を入力します。 ステップ1.4:アップロードトラフィックをブロックするWebサイトのドメインまたはサブドメイン（あるいはその両方）を定義します（この例ではcisco.localとそのすべてのサブドメインです）。 ステップ1.5:変更を送信します。 

	イメージ – カスタムURLカテゴリの作成 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-cu...
ステップ2:URLのトラフィックを復号化します。	注意：大量のURLを復号化すると、パフォーマンスが低下する可能性があります。 ステップ 2.1： GUIから、Web Security Managerに移動し、chooseDecryption 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Nameを入力します。 ステップ2.4.（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。 ヒント:（オプション）すべてのユーザが認証されていない場合でもポリシーを適用する場合は、All Users (authenticated and unauthenticated users)を選択します。 ステップ2.5: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：復号化ポリシーの作成

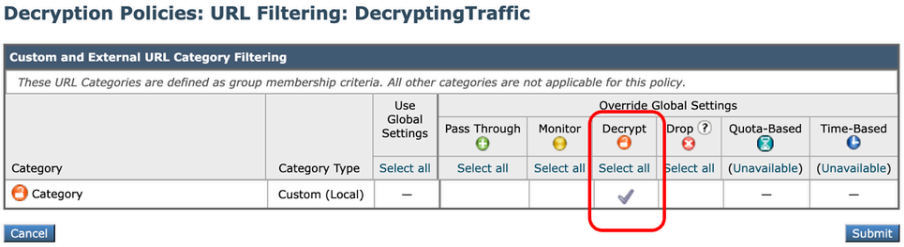
ステップ2.8:InDecryption Policies ページで、新しいポリシーのfromURL Filtering リンクをクリックします。

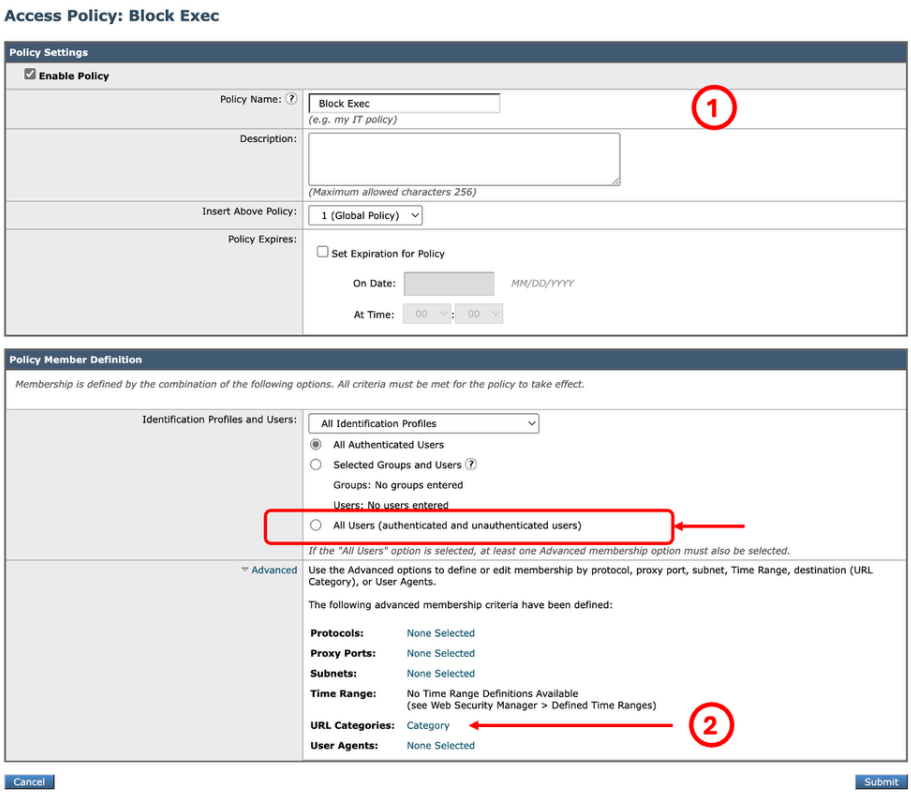


イメージ：URLフィルタリングの選択

ステップ2.9：カスタムURLカテゴリのアクションとしてChooseDecryptを使用します。

ステップ2.10:ClickSubmitをクリックします。



	イメージ – アクションとして復号化を設定
ステップ3:実行可能ファイルのブロック	ステップ3.1:GUIから、Web Security Managerに移動し、Access Policiesを選択します。 ステップ3.2:Add Policyをクリックします。 ステップ3.3：新しいポリシーのNameを入力します。 ステップ3.4.（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。 ヒント:（オプション）すべてのユーザが認証されていない場合でもポリシーを適用する場合は、All Users (authenticated and unauthenticated users)を選択します。 ステップ3.5:ポリシーメンバー定義の使用」セクションで、URLカテゴリの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3.6: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3.7:ClickSubmitをクリックします。  イメージ – アクセスポリシー

ヒント：レポート目的のために、他のアクセス/復号化ポリシーと同じではない名前を選択するのが最善です。

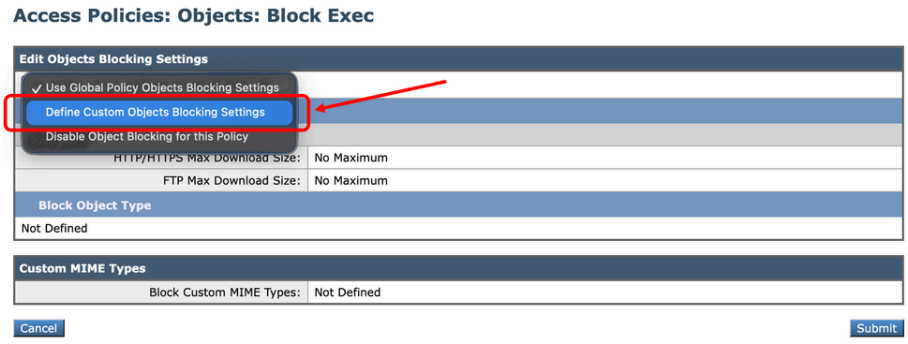
ステップ3.8:InAccess Policiesページで、URL FilteringアクションがMonitorに設定されていることを確認します。

ステップ 3.9： Access Policiesページで、新しいポリシーのObjectsからのリンクをクリックします。

イメージ – オブジェクトを選択

イメージ：URLフィルタリングの選択

ステップ 3.10： ドロップダウンメニューから、Define Custom Objects Blocking Settingsの順に選択します。

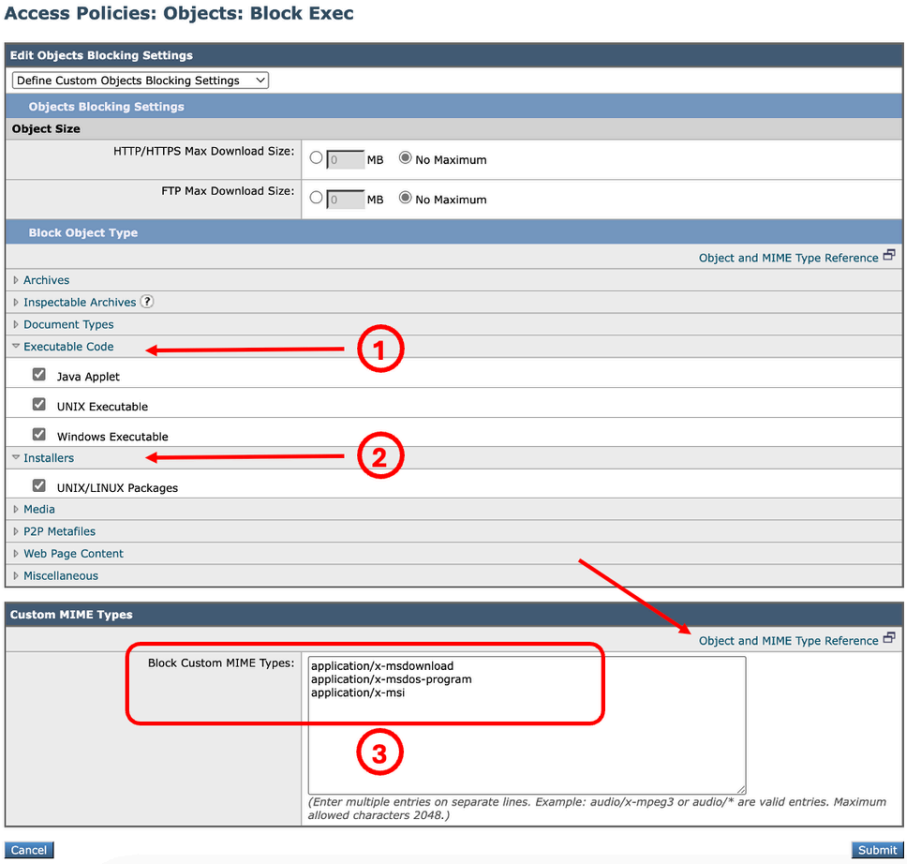


イメージ – カスタムオブジェクトを定義

ステップ3.11:ClickExecutable Codeを使用して、ブロックするオブジェクトのタイプを選択します。

ステップ3.12:インストーラをクリックして、ブロックするオブジェクトのタイプを選択します。

ステップ 3.13：また、「カスタムMIMEタイプ」セクションにブロックするファイルのMIMEタイプを入力することもできます。



イメージ：ブロックするオブジェクトの設定

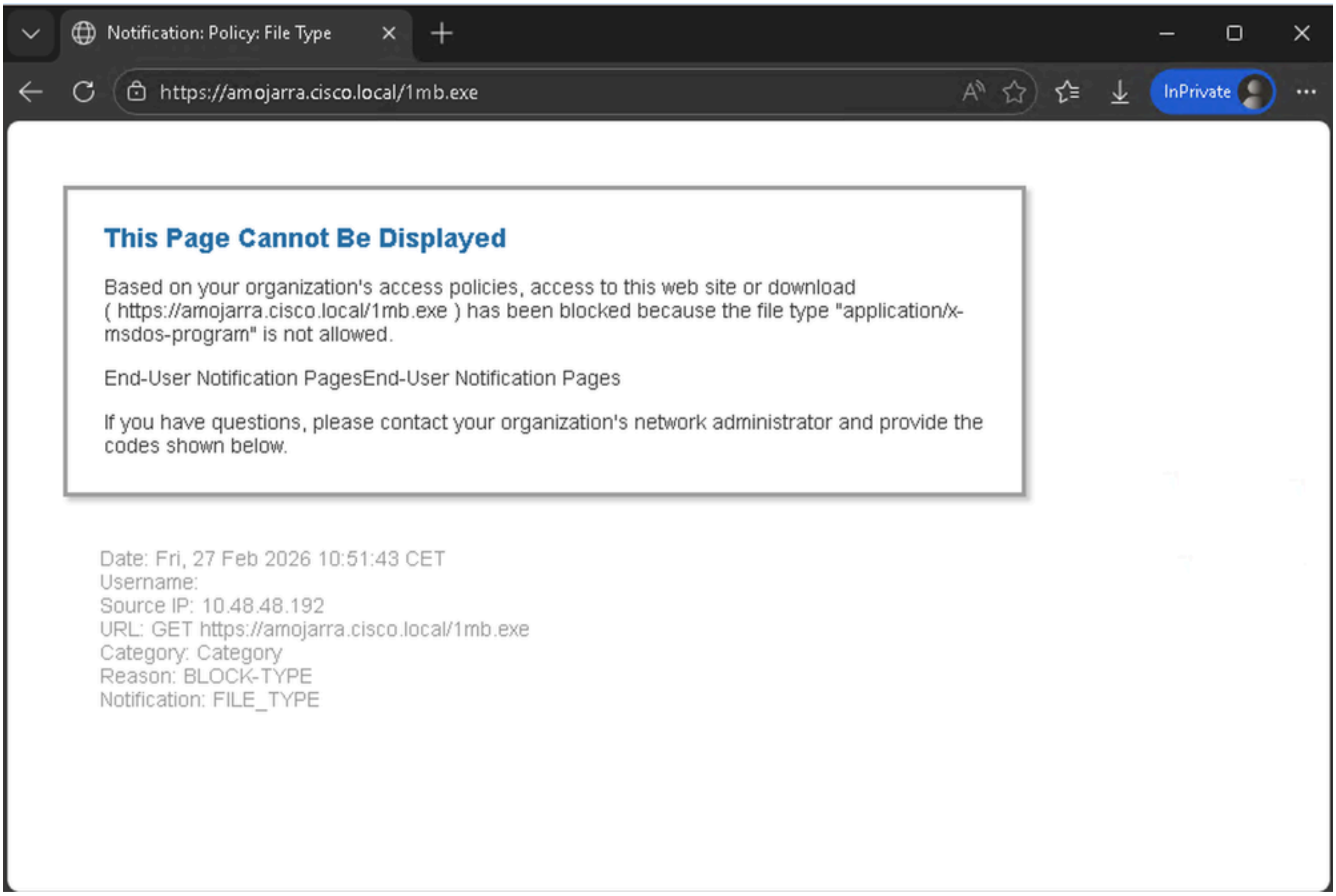
ヒント:MIMEタイプのリストを表示するには、オブジェクトおよびMIMEタイプのリファレンスをクリックします。

ステップ3.14:送信。

ステップ3.15:変更を確定します。

ファイル拡張子ブロックの検証

この例では、ユーザが実行可能ファイルをダウンロードしようとすると、次の警告ページが表示されます。



イメージ – ブロック通知ページ

ヒント：エンドユーザ通知(EUN)ページを設定するには、GUIからSecurity Servicesに移動し、End-User Notificationをクリックして End-User Notification Pagesセクションを変更します。

アクセスログから、トラフィックに関連する2つのログ行を確認できます。

最初のログ行は、トラフィックを復号する復号ポリシー(名前：DecryptingTraffic)に関連しています。アクションはDECRYPT_CUSTOMCAT

2番目のアクセスログ行は、手順3で作成したアクセスポリシー(名前：Block_Exec)に関連しています。アクションはBLOCK_ADMIN_FILE_TYPE

ポリシー	アクセスログ
復号化ポリシー	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",-,-,"-,"-,-,-","-," ",-,-,"-",-,"-","-,"-,"-,"-,"-","-","-","-","-","-","-",",1.71,0,-,"-","-","-","-","-","-,",-,"-,"-","-","-,","-,","-,",,"-,",-,"-,"-,","-,"-,","-,","-,",","- ","","",,

アクセスポリシー	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",0 "-",0,0,0,-"-",-,-,"-",-,"-","-","-","-","-",-,-,"nc",-,"","-","-","不明","不明","-","-",0.00,0,-,"不明","-","-","-","-","-","-","-",> -

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。