セキュアWebアプライアンスでのアップロードトラフィックのブロック

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)の特定のWebサイトへのアップロードトラフィック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。

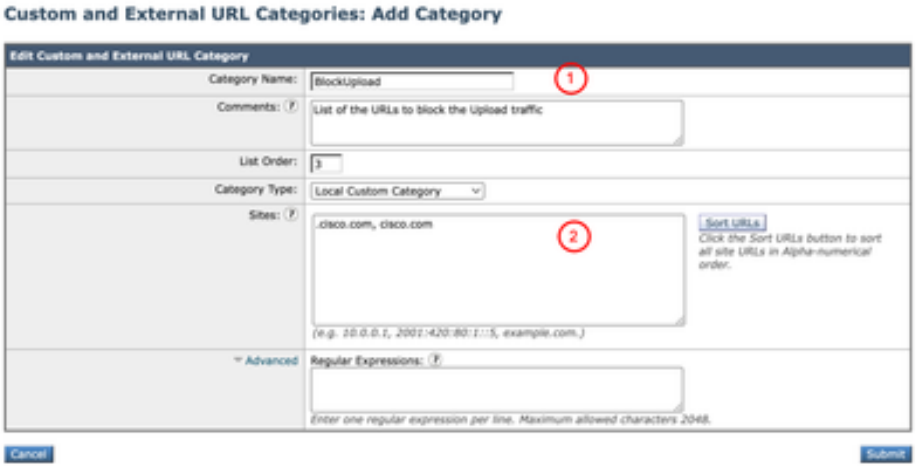
- SWAのグラフィックユーザインターフェイス(GUI)へのアクセス
- SWAへの管理アクセス。

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。

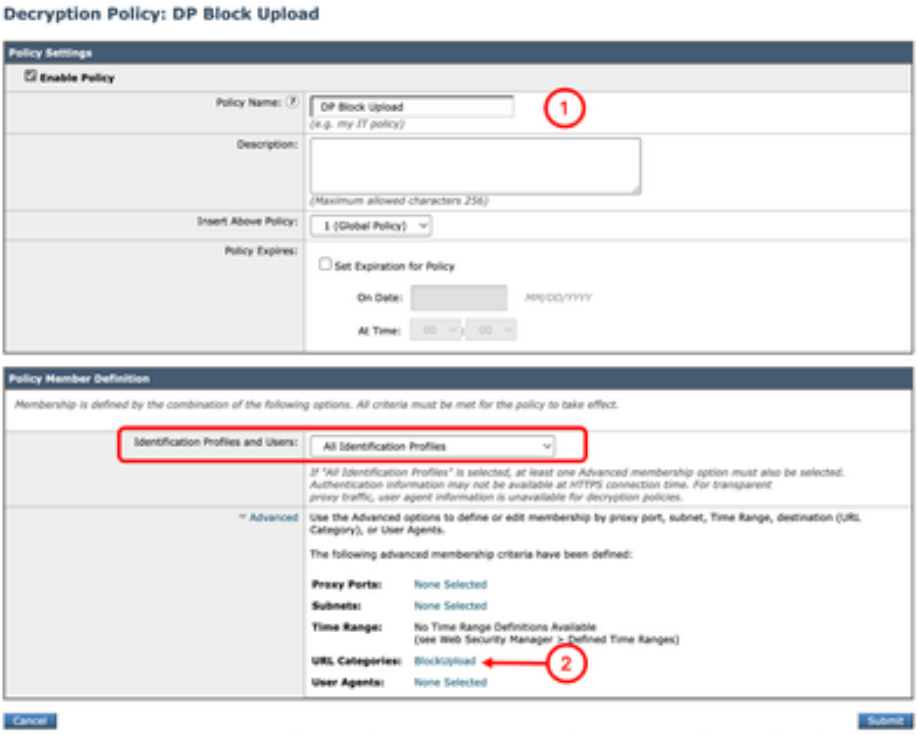
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定手順

ステップ 1：WebサイトのカスタムURLカテゴリを作成します。	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。 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：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.comとそのサブドメインすべて)。 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-custom-url-categories-in-secur.html
ステップ 2：URLの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.（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 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。



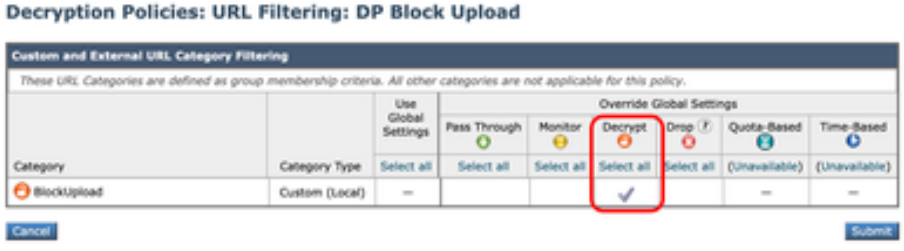
イメージ：復号化ポリシーの作成

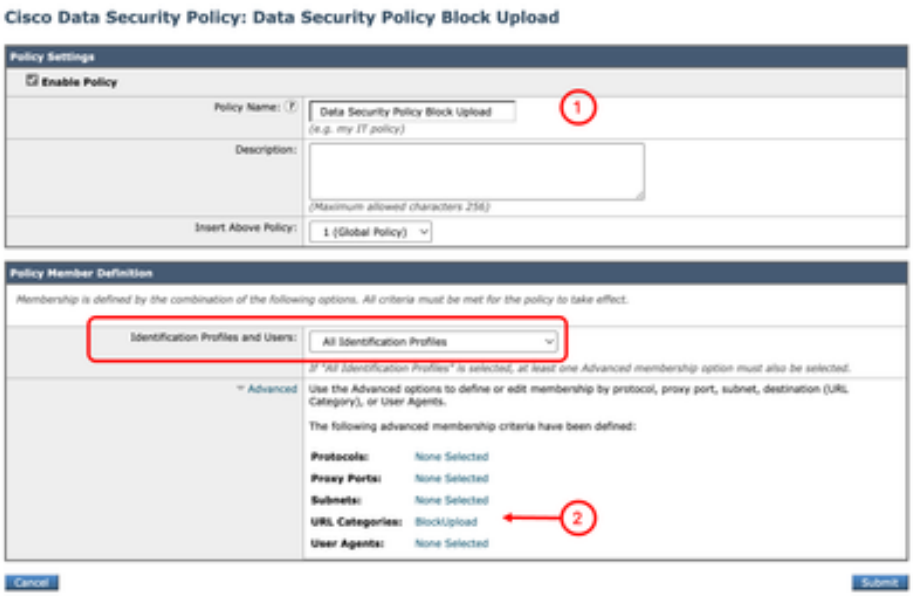
ステップ 2.8：Decryption Policiesページで、新しいポリシーに対するURL Filteringからのリンクをクリックします。

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復号化を選択します。

ステップ 2.10：[Submit] 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：アップロードトラフィックのブロック	ステップ 3.1：GUIで、Web Security Managerに移動し、Cisco Data Security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：新しいポリシーの名前を入力します。 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。 ステップ 3.5：ポリシーメンバー定義セクションで、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：[Submit] をクリックします。  図 – Cisco Data Security Policy 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：Cisco Date Security Policyページで、新しいポリシーのURL Filteringからの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 3.9：カスタムURLカテゴリのアクションとしてBlockを選択します。

ステップ 3.10：[Submit] をクリックします。

イメージ – ブロックアップロード

ステップ 3.11：変更を確定します。

レポートとログ

ログ

CLIからアップロードトラフィックに関連するログを表示するには、idsdataloss_logs(データセキュリティログのデフォルトのロギング名)を選択します。

ログにアクセスするには、次の手順を使用します。

ステップ 1：CLIにログインします

ステップ 2：grepと入力してEnterキーを押します。

ステップ 3：idsdataloss_logsに関連付けられている番号を検索して入力します。

- タイプ：「Data Security Logs」
- Retrieval: FTP Poll と入力し、Enterキーを押します。

ステップ4:（オプション）正規表現を入力してgrepし、キーワードでファンフィルタするか、Enterキーを押してすべてのログを表示します

ステップ5.（オプション）この検索で大文字と小文字を区別しますか？[Y]> ステップ4でキーワードを選択した場合は、大文字と小文字を区別しないフィルタを選択できます。

ステップ6.（オプション）一致しない行を検索しますか？[N]>ステップ4で定義した選択したキーワードを除くすべてのログをフィルタする必要がある場合は、このセクションを使用できます。そうでない場合は、Enterキーを押します。

ステップ7.（オプション）ログを追跡しますか？[N]>ライブログを表示する必要がある場合は、Yと入力してEnterキーを押します。それ以外の場合は、Enterキーを押して使用可能なログをすべて表示します。

ステップ8:（オプション）出力のページを分割しますか？[N]> ページごとに結果を確認する必要がある場合は、Y と入力してEnterキーを押すか、Enterキーを押してデフォルト値[N]を使用します。

レポート

Webトラッキングレポートを生成して、シスコデータセキュリティポリシー名でブロックされたアップロード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。

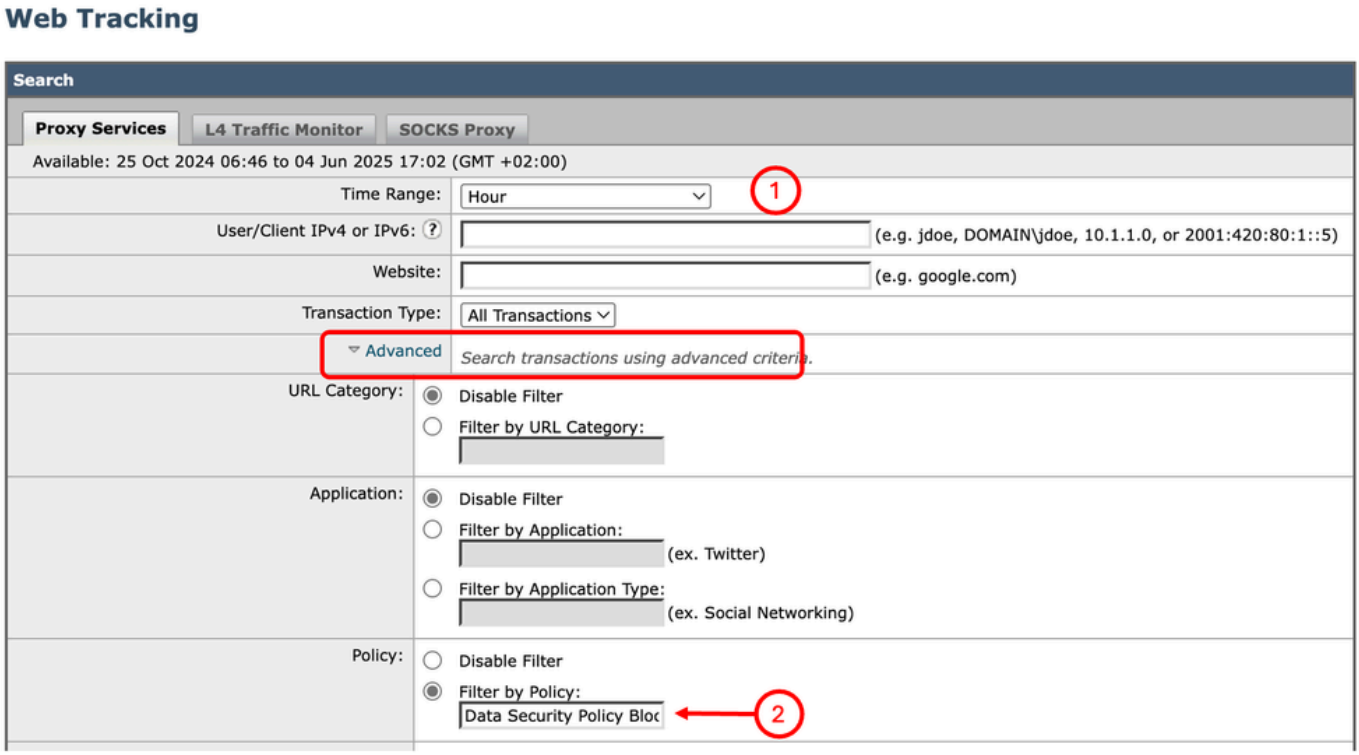
ステップ 1：GUIで、Reporting を選択し、Web Trackingを選択します。

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Cisco Data Security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。



イメージ：Webトラッキングレポートのフィルタリング

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 Appliances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。