Secure Web Applianceでの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)でトラフィックをブロックする手順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管理。

Cisco では次の前提を満たす推奨しています。

- 物理または仮想SWAがインストールされている。
- SWAグラフィカルユーザインターフェイス(GUI)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。

トラフィックのブロック

SWAでのトラフィックのブロックは、ネットワークセキュリティを確保し、内部ポリシーへのコンプライアンスを維持し、悪意のあるアクティビティから保護するための重要なステップです。トラフィックをブロックする一般的な理由を次に示します。

発信元によるブロッキングの理由

- 単一ユーザまたは複数ユーザによるフラッディング：1人または複数のユーザが大量のトラフィックを生成すると、ネットワークに過大な負荷がかかり、パフォーマンスの低下やサービスの中断を引き起こす可能性があります。
- アプリケーションによる信頼できないリソースアクセス (ユーザエージェント) :特定のアプリケーションが、信頼できないリソースや有害な可能性のあるリソースへのアクセスを試みる可能性があります。これらのユーザエージェントをブロックすると、セキュリティ違反やデータの漏洩を防ぐことができます。
- 特定のIP範囲に対するインターネットアクセスの制限：一部のIPアドレスまたは範囲は、セキュリティポリシーや不正な使用を防ぐために、インターネットへのアクセスを制限する必要があります。
- 疑わしいトラフィックの動作：悪意のあるアクティビティやセキュリティの脅威を示す可能性がある異常なパターンや動作を示すトラフィックは、ネットワークを保護するためにブロックする必要があります。

宛先によるブロッキングの理由

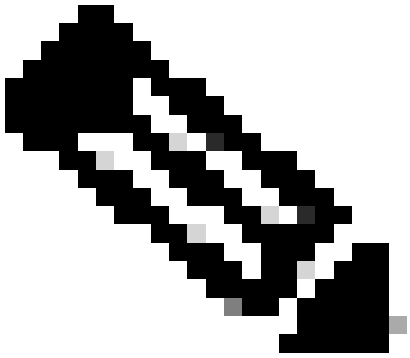
- 社内ポリシーの遵守：組織では、生産性を確保し、法規制を遵守するために、特定のWebサイトやオンラインリソースへのアクセスを制限するポリシーを設けていることがよくあります。
- 信頼できないサイト：信頼できないWebサイトや有害な可能性のあるWebサイトへのアクセスをブロックすると、フィッシング、マルウェア、およびその他のオンライン脅威からユーザを保護するのに役立ちます。
- 悪意のある動作：セキュリティ上の問題やデータ侵害を防ぐために、悪意のあるコンテンツをホストしたり、有害なアクティビティを実行したりするサイトをブロックする必要があります。

.

トラフィックをブロックする手順

一般に、SWAでトラフィックをブロックするには、次の3つの主要な段階があります。

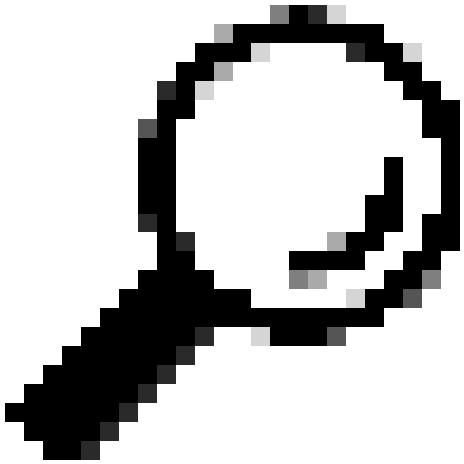
- ユーザのIDプロファイルを作成します。
- 復号化ポリシーでHTTPSトラフィックをブロックします。
- アクセスポリシーでHTTPトラフィックをブロックします。

ステージ	特定のユーザによるWebサイトへのアクセスをブロックする	特定のユーザによる特定のWebサイトへのアクセスをブロックする
カスタムURLカテゴリ	該当なし.	アクセスをブロックするサイトのカスタムURLカテゴリを作成します。 詳細については、次を参照してください。 Secure Web Applianceでのカスタム URLカテゴリの設定：シスコ
識別プロファイル	ステップ 1：GUIから、Web Security Managerを選択し、Identification Profilesをクリックします。 ステップ 2：Add Profileをクリックして、プロファイルを追加します。 ステップ 3：このプロファイルを有効にする、または削除せずにすばやく無効にするには、Enable Identification Profileチェックボックスを使用します。 ステップ 4：一意のプロファイル名を割り当てます。 ステップ5:（オプション）説明を追加します。 手順 6：Insert Aboveドロップダウンリストから、このプロファイルをテーブルのどこに表示するかを選択します。 手順 7： User Identification Methodセクションで、Exempt from authentication/ identificationを選択します。 ステップ 8：サブネットによるメンバーの定義で、この識別プロファイルを適用する必要があるIPアドレスまたはサブネットを入力します。IPアドレス、クラスレスドメイン間ルーティング(CIDR)ブロック、およびサブネットを使用できます。	 注：すべてのユーザに対して特定のWebサイトへのアクセスをブロックするために、個別のIDプロファイルを作成する必要はありません。これは、Global Decryption/Access Policyを使用して効率的に管理できます。 ステップ 1：GUIから、Web Security Managerを選択し、Identification Profilesをクリックします。 ステップ 2：Add Profileをクリックして、プロファイルを追加します。 ステップ 3：このプロファイルを有効にする、または削除せずにすばやく無効にするには、Enable Identification Profileチェックボックスを使用します。 ステップ 4：一意のプロファイル名を割り当てます。

		ステップ5: (オプション) 説明を追加します。 手順 6：Insert Aboveドロップダウンリストから、このプロファイルをテーブルのどこに表示するかを選択します。 手順 7： User Identification Methodセクションで、Exempt from authentication/ identificationを選択します。 ステップ 8：サブネットによるメンバーの定義で、この識別プロファイルを適用する必要があるIPアドレスまたはサブネットを入力します。IPアドレス、クラスレスドメイン間ルーティング(CIDR)ブロック、およびサブネットを使用できます。 ステップ 9： Advancedをクリックして、アクセスをブロックするURL Categoryを追加します。
復号化ポリシー	ステップ 1：GUIで、Web Security Managerを選択し、Decryption Policyをクリックします。 ステップ 2： Add Policyをクリックして、復号ポリシーを追加します。 ステップ 3：Enable Policyチェックボックスを使用して、このポリシーを有効にします。 ステップ 4：一意のポリシー名を割り当てます。 ステップ5: (オプション) 説明を追加します。 手順 6：Insert Above Policyドロップダウンリストから、最初のポリシーを選択します。 手順 7：Identification Profiles and Usersから、前の手順で作成したIdentification Profileを選択します。 ステップ 8：[Submit] をクリックしま	ステップ 1：GUIで、Web Security Managerを選択し、Decryption Policyをクリックします。 ステップ 2： Add Policyをクリックして、復号ポリシーを追加します。 ステップ 3：Enable Policyチェックボックスを使用して、このポリシーを有効にします。 ステップ 4：一意のポリシー名を割り当てます。 ステップ5: (オプション) 説明を追加します。 手順 6：Insert Above Policyドロップダウンリストから、最初のポリシーを選択します。 手順 7：Identification Profiles and Usersから、前の手順で作成したIdentification Profileを選択します。 ステップ 8：[Submit] をクリックしま

す。

ステップ 9：Decryption PoliciesページのURL Filteringの下で、この新しい復号ポリシーに関連付けられているリンクをクリックします。



ヒント：すべてのURLカテゴリをブロックしている場合は、カスタムURLカテゴリを削除し、事前定義されたURLカテゴリのみを使用して、ポリシーを最適化できます。これにより、URLをカスタムURLカテゴリと照合する追加の手順が不要になり、SWAの処理負荷が軽減されます。

ステップ 10：各URLカテゴリのアクションとしてDropを選択します。

ステップ 11 同じページで、Uncategorized URLsまでスクロールダウンし、ドロップダウンリストからDropを選択します。

ステップ 12[Submit] をクリックします。

イメージ – 特定のユーザのすべてのWebサイトをブロックする復号化ポリシー

す。

ステップ 9： Decryption PoliciesページのURL Filteringの下で、この新しい復号ポリシーに関連付けられているリンクをクリックします。

ステップ 10：ブロックされたWebサイト用に作成したカスタムURLカテゴリのアクションとしてDropを選択します。

ステップ 11[Submit] をクリックします。

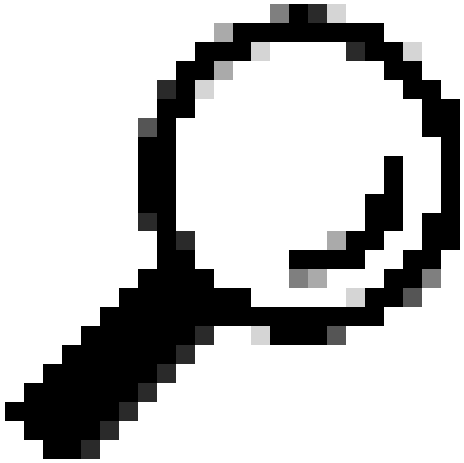
図 – 復号化ポリシーでのいくつかのURLのブロック

アクセスポリシー	ステップ 1：GUIから、Web Security Managerを選択し、Access Policyをクリックします。 ステップ 2： Add Policyをクリックして、アクセスポリシーを追加します。 ステップ 3：Enable Policyチェックボックスを使用して、このポリシーを有効にします。 ステップ 4：一意のポリシー名を割り当てます。 ステップ5:（オプション）説明を追加します。 手順 6：Insert Above Policyドロップダウンリストから、最初のポリシーを選択します。 手順 7：Identification Profiles and Usersから、前の手順で作成したIdentification Profileを選択します。 ステップ 8：[Submit] をクリックします。 ステップ 9：Access Policiesページの Protocols and User Agentsの下で、この新しいアクセスポリシーに関連付けられているリンクをクリックします。 ステップ 10： Edit Protocols and User Agents Settings ドロップダウンリストで、Define Custom Settingsを選択します。 ステップ 11イン ブロックプロトコルは、 両方のチェックボックス FTP over HTTPおよびHTTP。 ステップ 12イン HTTP CONNECTポートの場合、すべてのポート番号を削除して、すべてのポートをブロックします。	ステップ 1：GUIから、Web Security Managerを選択し、Access Policyをクリックします。 ステップ 2： Add Policyをクリックして、アクセスポリシーを追加します。 ステップ 3：Enable Policyチェックボックスを使用して、このポリシーを有効にします。 ステップ 4：一意のポリシー名を割り当てます。 ステップ5:（オプション）説明を追加します。 手順 6：Insert Above Policyドロップダウンリストから、最初のポリシーを選択します。 手順 7：Identification Profiles and Usersから、前の手順で作成したIdentification Profileを選択します。 ステップ 8：[Submit] をクリックします。 ステップ 9： Access Policiesページの URL Filteringの下で、この新しいアクセスポリシーに関連付けられているリンクをクリックします ステップ10:ブロックされたWebサイト用に作成したカスタムURLカテゴリのアクションとしてブロックを選択します。 ステップ 11[Submit] をクリックします。 ステップ 12変更を確定します。  イメージ：アクセスポリシーでのいくつかのURLのブロック

図 – アクセスポリシーでのプロトコルのブロックとポートの接続

ステップ 13[Submit] をクリックします。

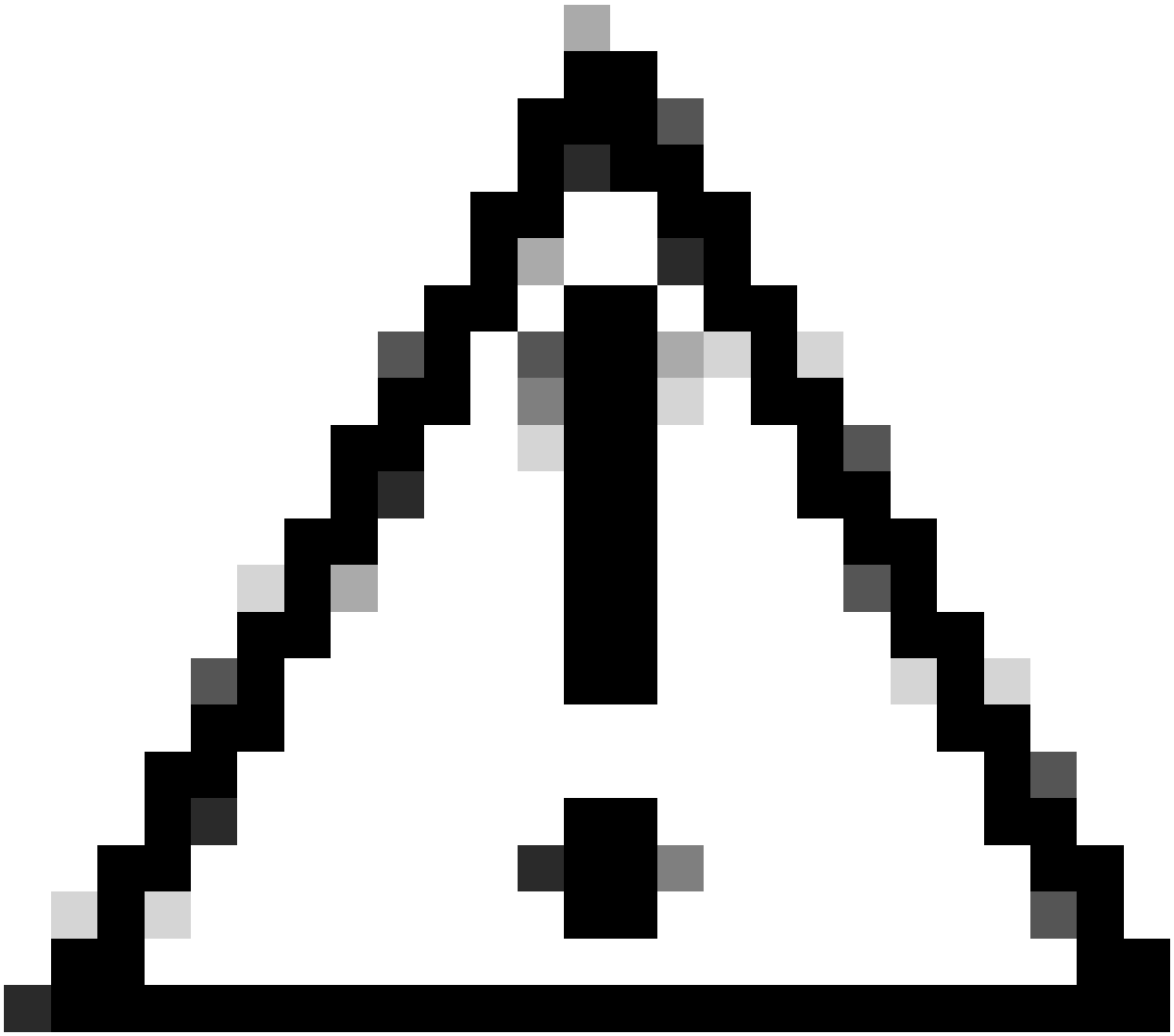
ステップ14（オプション）アクセスポリシーページのURLフィルタリングで、この新しいアクセスポリシーに関連付けられているリンクをクリックし、 すべてのURLカテゴリのアクションとしてBlockを選択し、 分類されていないURLがある場合は、Submitをクリックします。



ヒント：すべてのURLカテゴリをブロックしている場合は、カスタムURLカテゴリを削除し、事前定義されたURLカテゴリのみを使用して、ポリシーを最適化できます。これにより、URLをカスタムURLカテゴリと照合する追加の手順が不要になり、SWAの処理負荷が軽減されます。

ステップ 16：変更を確定します。

	 イメージ：すべてのサイトをブロックするアクセスポリシー	



注意：透過的なプロキシ導入では、トラフィックが復号化されない限り、SWAはユーザエージェントまたはHTTPSトラフィックのフルURLを読み取ることができません。その結果、ユーザエージェントまたは正規表現を使用するカスタムURLカテゴリを使用して識別プロファイルを設定する場合、このトラフィックは識別プロファイルの照合に失敗します。

透過型プロキシ導入での正規表現を使用したサイトのブロック

トランスペアレントプロキシ導入で、正規表現の条件を持つカスタムURLカテゴリをブロックす

る予定の場合（たとえば、一部のYouTubeチャンネルへのアクセスをブロックする場合）、次の手順を使用できます。

ステップ 1：メインサイトのカスタムURLカテゴリを作成します。(この例ではYouTube.com)。

ステップ 2：復号化ポリシーを作成し、このカスタムURLカテゴリを割り当て、アクションを復号化に設定します。

ステップ 3：アクセスポリシーを作成し、正規表現（この例ではYouTubeチャネルのカスタムURLカテゴリ）にカスタムURLカテゴリを割り当て、アクションをブロックに設定します。

関連情報

- AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド – GD(General Deployment) – ポリシーアプリケーションのエンドユーザの分類[Cisco Secure Web Appliance] – シスコ
- Secure Web Applianceでのカスタム URLカテゴリの設定：シスコ
- Cisco Webセキュリティアプライアンス(WSA)でOffice 365トラフィックを認証および復号化から除外する方法：シスコ

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。