Secure Web ApplianceでのMicrosoft Updatesトラフィックのバイパス

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)でMicrosoft Updates(MUPDATE)トラフィックをバイパス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。

次のツールをインストールすることをお勧めします。

- 物理または仮想SWA
- 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。

Microsoftの更新

Microsoftの更新プログラムは、オペレーティングシステムおよびソフトウェアアプリケーションに関してMicrosoftがリリースした必須のパッチ、セキュリティアップデート、および機能拡張です。これらの更新は、コンピュータとネットワークデバイスのセキュリティ、安定性、およびパフォーマンスを維持するために不可欠です。システムを脆弱性から保護し、バグを修正し、新機能や改良をソフトウェアに統合します。

Cisco SWAなどのプロキシサーバに対するMicrosoftアップデートの影響は大きい可能性があります。これらの更新には、大きなファイルや多数の小さなファイルのダウンロードが含まれることが多く、プロキシの帯域幅と処理リソースを大量に消費する可能性があります。これは、輻輳、ネットワークパフォーマンスの低下、プロキシインフラストラクチャの負荷の増大を引き起こし、ユーザエクスペリエンス全体やその他の重要なネットワーク運用に影響を与える可能性があります。

プロキシからMicrosoft Updateトラフィックをバイパスすることは、これらの課題を管理するための安全で効果的な方法です。Microsoftアップデートは信頼できるMicrosoftサーバから発信されるため、このトラフィックがプロキシをバイパスするようにすると、ネットワークセキュリティを損なうことなくプロキシサーバの負荷を軽減できます。これにより、重要な更新が効率的に配信されると同時に、他のセキュリティおよびコンテンツフィルタリングタスク用のプロキシリソースが保持されます。ただし、このようなバイパス設定を慎重に実装して、ネットワーク全体のセキュリティと組織のポリシーへのコンプライアンスを維持することが重要です。

Microsoft更新プログラムのバイパス

Microsoft Updatesトラフィックのプロキシを回避することを検討している場合、主に2つのアプローチがあります

1. バイパス：これには、トラフィックがSWAに到達しないようにトラフィックをリダイレクトするようにネットワークを設定することが含まれます。
2. パススルー：これには、Microsoft Updatesトラフィックを復号化もスキャンもしないようにSWAを設定し、インスペクションなしでプロキシをパススルーできるようにする作業が含まれます。

SWAでのトラフィックのバイパス

SWAが装備されたネットワークでMicrosoft Updatesトラフィックをバイパスする方法は、プロキシ導入の設定によって異なります。

導入タイプ	トラフィックのバイパス
透過的な導入	トラフィックをプロキシサーバに転送する役割を担うルータまたはレイヤ4スイッチで、Microsoft Updatesトラフィック

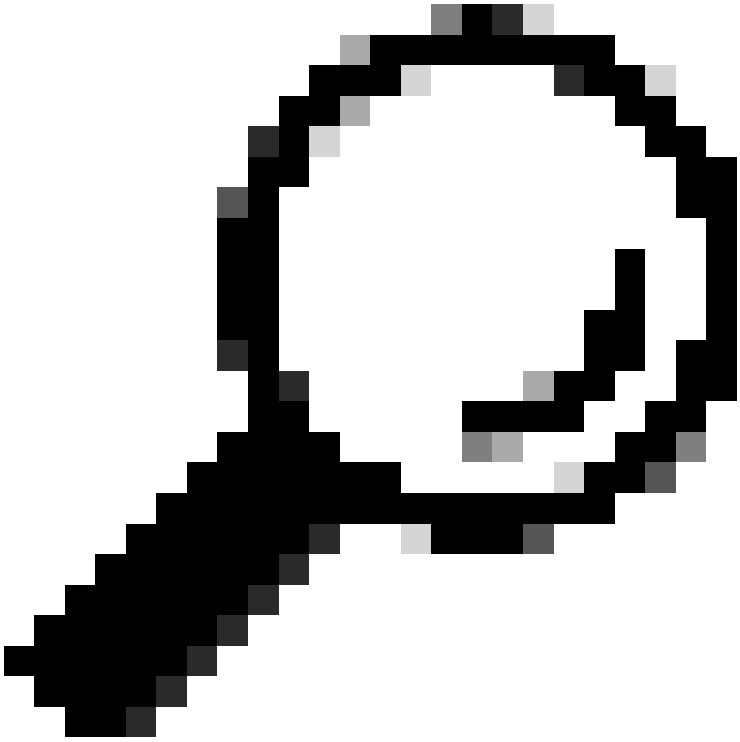
	をリダイレクトできます。
	バイパス設定は、SWAのグラフィカルユーザインターフェイス(GUI)で直接設定できます。
明示的な展開	Microsoft UpdatesトラフィックがSWAに到達しないようにするには、送信元でバイパスを設定する必要があります。これは、トラフィックがSWAにリダイレクトされないように、クライアントマシンで関連URLを除外することを意味します。

特定のトラフィックをバイパスするために広範なネットワーク再設計が必要で、それが不可能な場合は、SWAを設定して特定のタイプのトラフィックを通過させる方法もあります。これは、指定されたトラフィックを復号化もスキャンもしないようにSWAを設定し、インスペクションなしでプロキシを通過できるようにすることで実現できます。この方法により、ネットワークパフォーマンスとプロキシリソースへの影響を最小限に抑えながら、重要なトラフィックを効率的に配信できます。

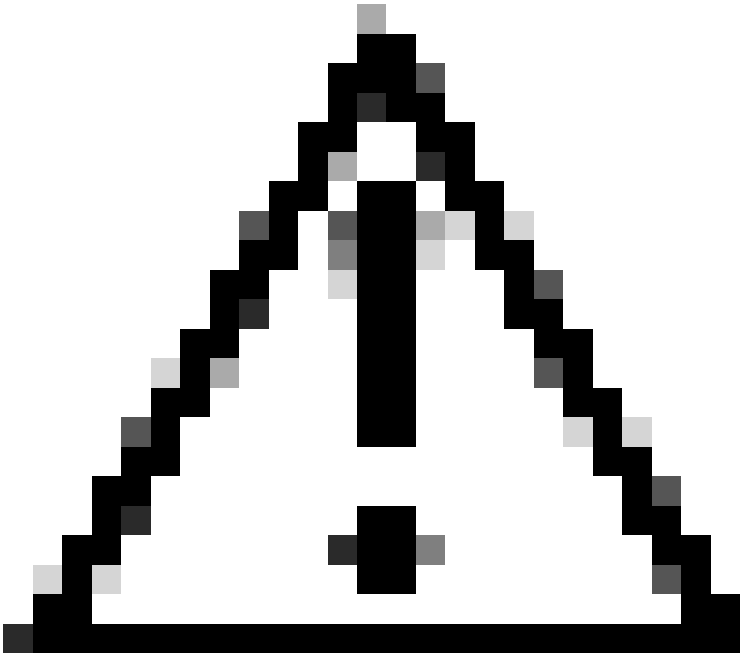
Microsoftアップデートのパススルー手順

Microsoft Updatesトラフィックのパススルーには、主に次の4つの段階があります。

段階	手順
1. Microsoft Updates URL用のカスタムURLカテゴリの作成	ステップ1:GUIで、Web Security Managerを選択し、カスタムおよび外部URLカテゴリをクリックします。 ステップ2：カスタムURLカテゴリを追加するには、ClickAddカテゴリをクリックします。 手順4:一意のCategoryName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：リスト順から、一番上に配置する最初のカテゴリを選択します。 手順 7：Category Typeドロップダウンリストから、Local Custom Categoryを選択します。 ステップ 8： SitesセクションにMicrosoft Updates URLを追加します。



ヒント:Microsoftの更新プログラムの一覧は、次のリンクから確認できます。手順2 - WSUSの構成 | Microsoftラーニング



注意:Microsoftのドキュメントにあるリンクをコピー/ペーストしないでください。SWA形式で正しくフォーマットしてください。 詳細については、次のサイト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 ステップ 9：[Submit] をクリックします。
2. Microsoft Updatesトラフィックを認証から除外するためのIDプロファイルの作成	ステップ10:GUIから、Web Security Managerを選択し、Identification Profilesをクリックします。 ステップ11：プロファイルを追加するには、Addプロファイルをクリックします。 ステップ12:Enable Identification Profileチェックボックスを使用して、このプロファイルを有効にするか、削除せずにすばやく無効にします。 ステップ13:一意のprofileNameを割り当てます。 ステップ14:（オプション）説明を追加します。 ステップ15:上記の挿入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内のどこに表示するかを選択します。 ステップ 16： ユーザ識別方法セクションで、認証/識別から免除を選択します。 手順17:「サブネットによるメンバーの定義」で、特定のユーザのためにMicrosoftトラフィックをパススルーする場合は、適用されるIPアドレスまたはサブネットを入力します。すべてのIPアドレスを含める場合は、このフィールドを空白のままにします。 ステップ 18：Advancedセクションで、Custom URL Categoriesを選択します。 ステップ 19：Microsoftのアップデート用に作成されたカスタムURLカテゴリを追加します。 ステップ 20：[Done] をクリックします。 ステップ 21： [Submit] をクリックします。
3. Microsoft Updatesトラフィックをパススルーするための復号化ポリシーの作成	ステップ22:FromGUI、ChooseWeb Security Manager、clickDecryption Policyの順に選択します。 ステップ 23： ClickAdd Policiesをクリックして、復号ポリシーを追加します。 ステップ24：このポリシーを有効にするには、Enable Policyチェックボックスを使用します。 ステップ25:一意のPolicyNameを割り当てます。

	ステップ26: (オプション) 説明を追加します。 ステップ27:Insert Above Policies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。 ステップ28:Identification Profiles and Usersから、前のステップで作成したIdentification Profileを選択します。 ステップ 29：[Submit] をクリックします。 ステップ30:復号ポリシーページのURLフィルタリングで、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32:SelectPassthroughには、Microsoft Updates URLカテゴリのアクションがあります。 ステップ 32：[Submit] をクリックします。
4. Microsoft Updatesトラフィックを許可するアクセスポリシーの作成	ステップ33:GUIから、Web Security Managerを選択し、Access Policyをクリックします。 ステップ 34： Add Policies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35：このポリシーを有効にするには、Enable Policyチェックボックスを使用します。 ステップ36:一意のPolicyNameを割り当てます。 ステップ37: (オプション) 説明を追加します。 ステップ38:Insert Above Policies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。 ステップ39:Identification Profiles and Usersから、前のステップで作成したIdentification Profileを選択します。 ステップ 40：[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:Microsoft Updatesに対して作成されたカスタムURLカテゴリのアクションとしてAllowas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。

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
- 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：シスコ
- セキュアWebアプライアンスでの認証のバイパス：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。