セキュアWebアプライアンスでの認証のバイパス

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)で認証を免除(Exempt)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。

認証の免除

Cisco SWAの特定のユーザまたはシステムの認証を免除することは、運用効率を維持し、特定の要件を満たすために非常に重要です。まず、一部のユーザまたはシステムは、認証プロセスによって妨げられる可能性がある重要なリソースまたはサービスへの中断のないアクセスを必要とします。たとえば、定期的な更新やバックアップを実行する自動化されたシステムやサービス・アカウントには、認証メカニズムによる遅延や障害の可能性のない、シームレスなアクセスが必要です。

また、Webサービスプロバイダーがプロキシを使用してサービスにアクセスしないことを推奨するシナリオもあります。このような場合、認証を除外することで、プロバイダーのガイドラインに確実に準拠し、サービスの信頼性を維持できます。さらに、特定のユーザのトラフィックを効果的にブロックするには、まずそのユーザを認証から除外し、適切なブロッキングポリシーを適用する必要があります。このアプローチにより、アクセス権限を正確に制御できます。

場合によっては、Microsoftの更新プログラムなど、アクセスされるWebサービスが信頼され、世界中で受け入れられます。このようなサービスの認証を免除すると、すべてのユーザのアクセスが簡素化されます。さらに、ユーザのオペレーティングシステムやアプリケーションがSWAで設定されている認証メカニズムをサポートしていない場合は、接続を確保するためにバイパスが必要になります。

最後に、ユーザログインがなく、制限付きの信頼できるインターネットアクセスを持つ固定IPアドレスを持つサーバは、アクセスパターンが予測可能で安全であるため、認証を必要としません。

これらのケースで認証を戦略的に除外することで、組織はセキュリティニーズと運用効率のバランスを取ることができます。

Cisco SWAの認証を免除する方法

SWAでの認証の免除は、それぞれ特定のシナリオと要件に合ったさまざまな方法で実現できます。認証例外を設定する一般的な方法を次に示します。

- IPアドレスまたはサブネットマスク：最も簡単な方法の1つは、特定のIPアドレスまたはサブネット全体を認証から除外することです。これは、インターネットまたは内部リソースへの中断のないアクセスを必要とする、固定IPアドレスまたは信頼されたネットワークセグメントを持つサーバに特に役立ちます。SWA設定でこれらのIPアドレスまたはサブネットマスクを指定することで、これらのシステムが認証プロセスをバイパスすることを確認できます。
- プロキシポート：特定のプロキシポートに基づいてトラフィックを除外するようにSWAを設定できます。これは、特定のアプリケーションまたはサービスが通信に指定ポートを使用する場合に便利です。これらのポートを特定することで、これらのポート上のトラフィックの認証をバイパスするようにSWAを設定し、関連するアプリケーションやサービスにシームレスなアクセスを提供できます。

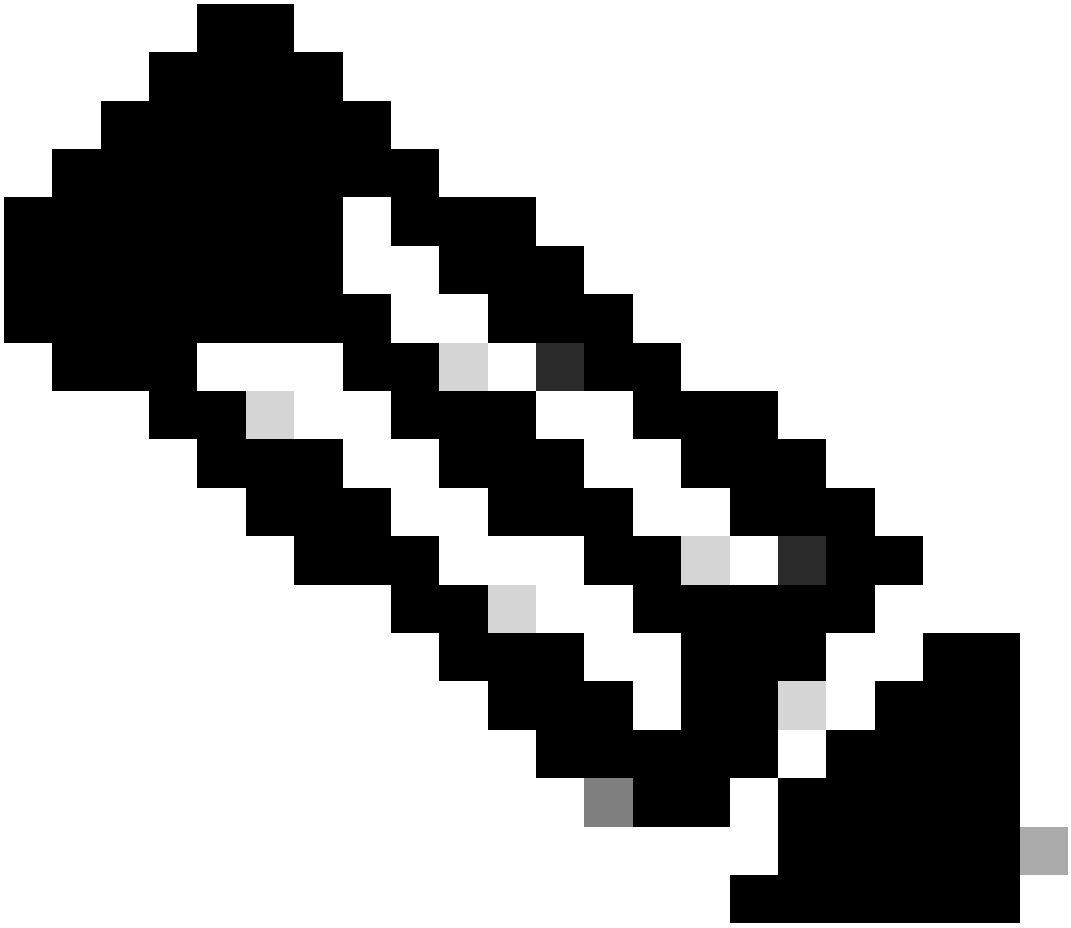
- URLカテゴリ：URLカテゴリに基づいて認証を免除する方法もあります。これには、定義済みのシスコカテゴリと、組織固有のニーズに基づいて定義したカスタムURLカテゴリの両方を含めることができます。たとえば、Microsoftの更新プログラムなど、特定のWebサービスが信頼され、一般的に受け入れられると見なされる場合、これらの特定のURLカテゴリの認証をバイパスするようにSWAを設定できます。これにより、すべてのユーザが認証を必要とせずにこれらのサービスにアクセスできます。
- ユーザエージェント：ユーザエージェントに基づく認証の免除は、設定された認証メカニズムをサポートしない特定のアプリケーションまたはデバイスを扱う場合に便利です。これらのアプリケーションまたはデバイスのユーザエージェント文字列を識別することで、SWAを設定して、それらのアプリケーションまたはデバイスから発信されるトラフィックの認証をバイパスし、シームレスな接続を確保できます。

.

認証をバイパスする手順

認証を免除するIDプロファイルを作成する手順は、次のとおりです。

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 the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。

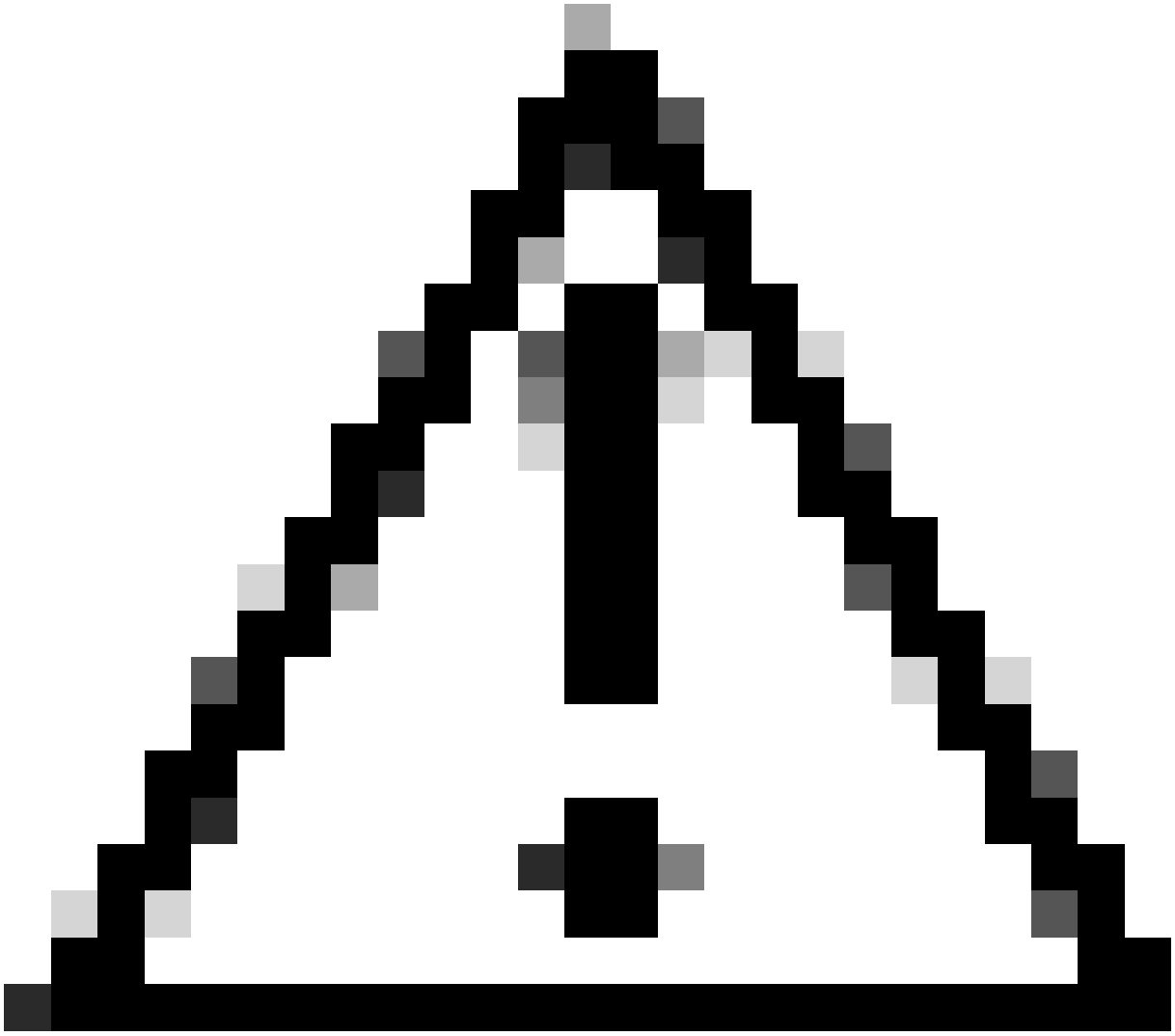


注：リストの一番上の認証を必要としない職位識別プロファイル。このアプローチにより、SWAの負荷が軽減され、認証キューが最小化されるため、他のユーザの認証が高速になります。

手順 7： User Identification Methodセクションで、Exempt from authentication/ identificationを選択します。

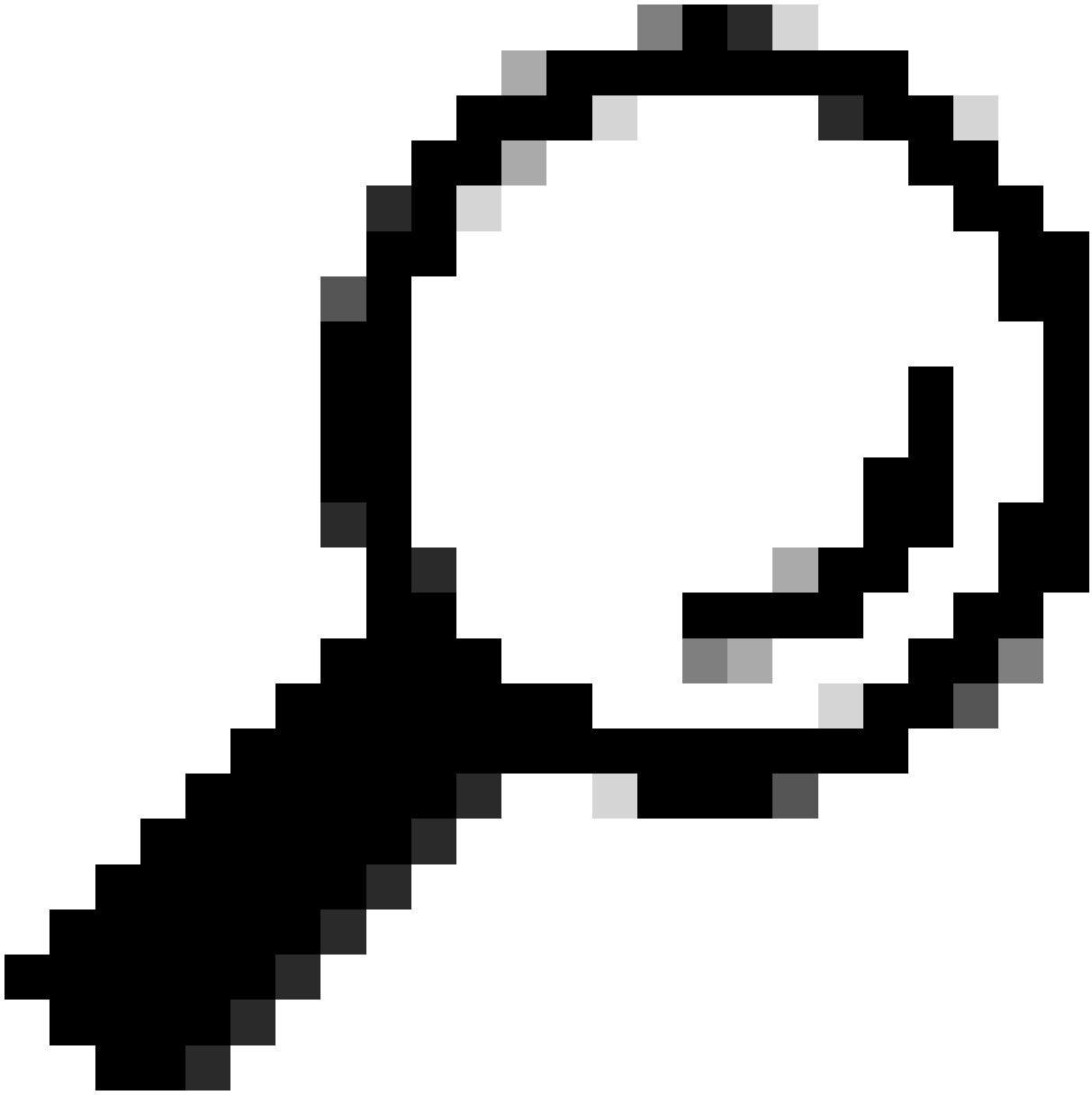
ステップ 8：サブネットによるメンバーの定義で、この識別プロファイルを適用する必要があるIPアドレスまたはサブネットを入力します。IPアドレス、クラスレスドメイン間ルーティング(CIDR)ブロック、およびサブネットを使用できます。

ステップ9: (オプション) Advancedをクリックして、Proxy Ports、URL Categories、User Agentsなどの追加メンバーシップ基準を定義します。

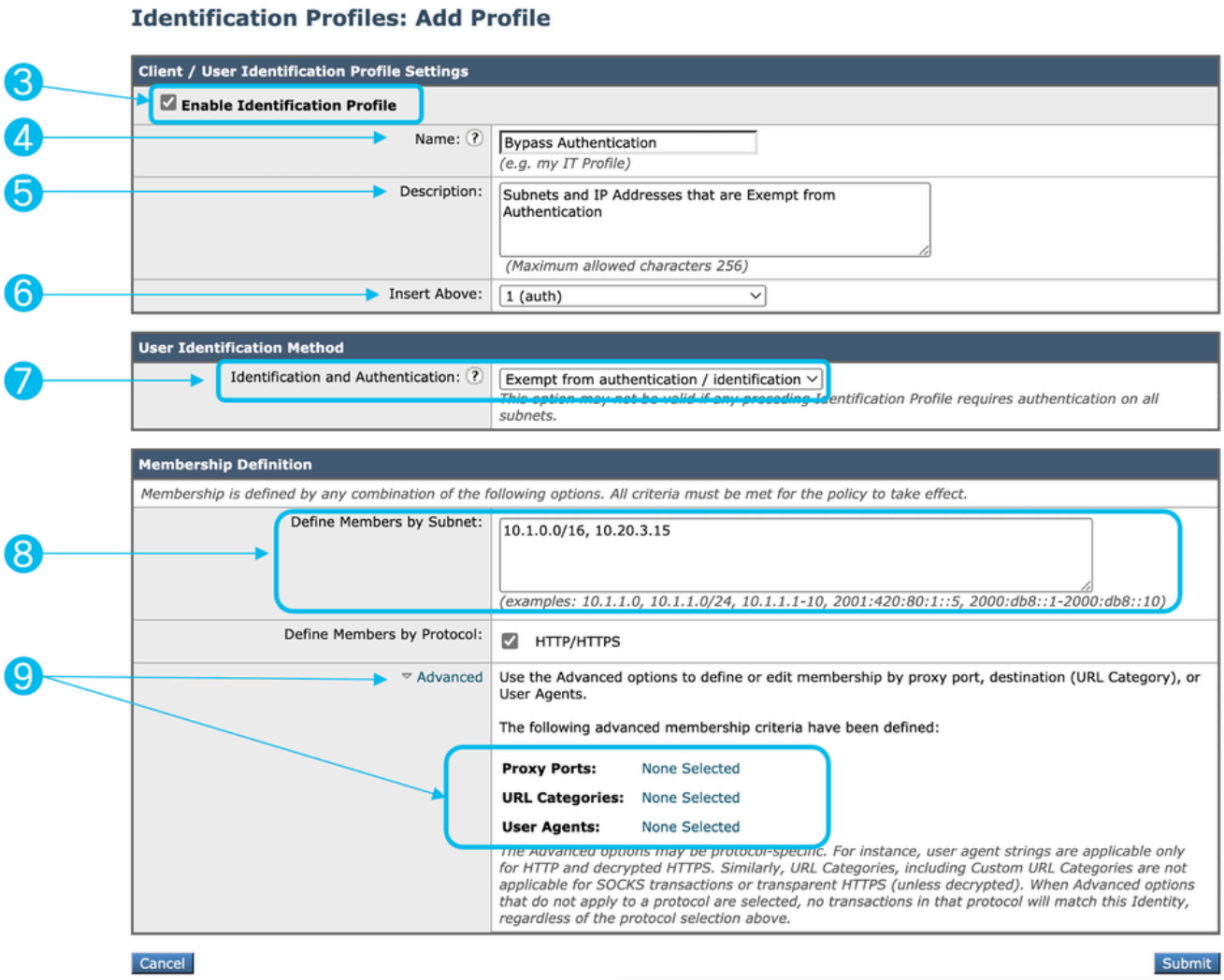


注意：透過的なプロキシ導入では、トラフィックが復号化されない限り、SWAはユーザエージェントまたはHTTPSトラフィックのフルURLを読み取ることができません。その結果、ユーザエージェントまたは正規表現を使用するカスタムURLカテゴリを使用して識別プロファイルを設定する場合、このトラフィックは識別プロファイルの照合に失敗します。

カスタムURLカテゴリの設定方法の詳細については、「Configure Custom URL Categories in Secure Web Appliance - Cisco



ヒント：ポリシーではAND口ジックが使用されています。つまり、IDプロファイルが一致するにはすべての条件を満たす必要があります。Advancedオプションを設定すると、ポリシーが適用されるすべての要件を満たす必要があります。



イメージ：認証をバイパスするためのIDプロファイルの作成手順

ステップ 10：送信し、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。