WSA でウイルス対策の保護を失うことなく WBRS の低いトラフィック フローを許可する

目次

概要

このドキュメントでは、ウィルス対策プログラムを使用したまま、Cisco Web セキュリティ アプライアンス（WSA）で Web ベース レピュテーション スコア（WBRS）が低いトラフィックを許可する方法を説明します。

前提条件

要件

WSA デバイスに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、AsyncOS Versions 5.6 以降が稼働する WSA デバイスに基づいています。

問題

WBRS が低いためにサイトがブロックされる。 トラフィックを許可したいが、引き続きウィルス対策プログラムでトラフィックをスキャンする必要もある。

解決策

この宛先へのトラフィックが許可されるようにするには、この要求と一致する特殊なアイデンテ

ィティ/アクセス ポリシーを作成します。 たとえば、**www.example.com** のスコアが -6.0 であるため、このサイトが現在ブロックされている場合、まず、この URL 用のカスタム URL カテゴリを作成します。 次に、新しく作成したカテゴリをアイデンティティにバインドし、そのアイデンティティをアクセス ポリシーにバインドします。そして最後に、アクセス ポリシーの WBRS ブロック範囲を変更します。

カスタム URL カテゴリを作成するには、次の手順に従います。

1. WSA にログインして [Web Security Manager] > [Custom URL categories] に移動し、[Add Custom Category...] をクリックします。

2. 次のようなエントリを作成します。

   [Category Name]： **Bypass.WBRS**[Sites]： **www.example.com**

3. 設定が完了したら、エントリを送信します。

新しいカテゴリをアイデンティティにバインドするには、次の手順に従います。

1. [Web Security Manager] > [Identities] に移動し、[Add Identity...] をクリックします。

2. 次のようなアイデンティティを作成します。

   [Name]： **Bypass.WBRS.id**[Insert Above]： **1**[Advanced URL Categories]： **Bypass WBRS**

3. 必要に応じて、他のフィールドを設定します。 たとえば、認証を要件とする場合、このアイデンティティに対して認証を有効にします。

4. 設定が完了したら、アイデンティティを送信します。

新しいアイデンティティをアクセス ポリシーにバインドするには、次の手順に従います。

1. [Web Security Manager] > [Access Policies] に移動し、[Add Policy...] をクリックします。

2. 次のようなポリシーを作成します。

   [Policy Name]： **Bypass.WBRS.policy**[Insert Above Policy]： **1**[Identities and Users]： **1 つ以上のアイデンティティを選択**[Identity]： **Bypass.WBRS.id**

3. 必要に応じて、他のフィールドを設定します。

4. 設定が完了したら、ポリシーを送信します。

この新しいアクセス ポリシーの WBRS ブロック範囲を変更するには、次の手順に従います。

1. [Web Security Manager] > [Access Policies] > [Bypass.WBRS.policy] > [Web Reputation and Anti-Malware Filtering] に移動し、[(global policy)] をクリックします。

2. [Web Reputation and Anti-Malware Settings] の選択項目を [Define Web Reputation and Anti-Malware Custom Settings] に変更します。 これにより、Web レピュテーションの設定を変更できるようになります。

3. [BLOCK Range] を指定する矢印を移動して、[-7.0] からブロックするように設定します。

ページがウィルスであり、そのスコアがさらに低い場合、全範囲でスキャンが行われないようにするために、このステップが必要となります。

4. 設定が完了したら、変更を送信して確定します。

以上の設定により、ユーザが **www.example.com** に要求を送信すると、WSA がその要求を **Bypass.WBRS.id** に割り当てます。 **Bypass.WBRS.id** には **Bypass.WBRS.policy** がバインドされているため、WSA は **Bypass.WBRS.policy** に設定されているポリシーを適用します。 このポリシーでの WBRS 設定は **-7.0** からブロックするように設定されているため、要求は許可されます。

注: Bypass.WBRS カテゴリを使用して URL カテゴリのアクションを [Allow] に設定すると、ウィルス対策/マルウェア スキャンがバイパスされます。 したがって、この場合はアクションを [Monitor] に設定してください。