

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決策](#)

概要

この資料に抗ウイルスプログラムの継続的使用の Cisco Web セキュリティ アプライアンス (WSA) を通して低い Web ベース 評判スコア (WBRs) とのトラフィックを許可する方法を記述されています。

前提条件

要件

Cisco は WSA デバイスのナレッジがあることを推奨します。

使用するコンポーネント

この文書に記載されている情報は AsyncOS バージョン 5.6 および それ 以降を実行する WSA デバイスで基礎です。

問題

サイトは下位 WBRs がブロックされた原因です。トラフィックを許可することを望みますがまだ抗ウイルスプログラムを用いるトラフィックをスキャンします。

解決策

この宛先にトラフィックを許可することを望む場合要求と一致する特別な識別を/アクセスポリシーを作成して下さい。たとえば、[www.example.com](#) に -6.0 のスコアがあり、現在ブロックされれば、最初にこの URL に対するカスタム URL カテゴリを作成して下さい。それから識別に新しいカテゴリを結合して下さいアクセスポリシーに識別を結合し、最終的にアクセスポリシーのための WBRs ブロック範囲を修正します。

カスタム URL カテゴリを作成するためにこれらのステップを完了して下さい:

1. WSA にログイン し、**Web セキュリティ マネージャ**に > **カスタム URL カテゴリ** ナビゲート し、『Add』 をクリック して下さい**カスタム カテゴリ**を....
2. これと同じようなエントリを作成して下さい:

カテゴリ名: **Bypass.WBRS**サイト: www.example.com

3. 設定が完了したエントリを入れて下さい。

識別に新しいカテゴリを結合 するためにこれらのステップを完了して下さい:

1. **Web セキュリティ マネージャ** > **識別**にナビゲート し、『Add』 をクリック して下さい**識別**を....
2. これと同じような識別を作成して下さい:

[Name] : **Bypass.WBRS.id**上で挿入して下さい: 1高度 URL カテゴリ: **バイパス WBRS**

3. 望まれるように他のフィールドを設定して下さい。たとえば認証を必要としたら、そしてこの識別のための認証を有効に して下さい。
4. 設定が完了した識別を入れて下さい。

アクセスポリシーに新しい識別を結合 するためにこれらのステップを完了して下さい:

1. **Web セキュリティ マネージャ** > **アクセスポリシー**にナビゲート し、『Add』 をクリック して下さい**ポリシー**を....
2. これと同じようなポリシーを作成して下さい:

ポリシー名: **Bypass.WBRS.policy**ポリシーの上で挿入して下さい: 1識別およびユーザ: 1つ以上の識別を選択して下さい識別: **Bypass.WBRS.id**

3. 望まれるように他のフィールドを設定して下さい。
4. 設定が完了したポリシーを入れて下さい。

この新しいアクセスポリシーのための WBRS ブロック範囲を修正するためにこれらのステップを完了して下さい:

1. **Web セキュリティ マネージャ** > **アクセスポリシー** > **Bypass.WBRS.policy** > **Web 評判および反Malware フィルタリング**にナビゲート し、クリックして下さい (**グローバル な ポリシー**)。
2. **Web 評判および反Malware カスタム 設定**を定義するために **Web 評判および反Malware 設定**選択を変更して下さい。これは Web 評判設定を変更することを可能にします。
3. -7.0 でブロックし始めるあるように**ブロック範囲**を規定し、それを設定した 矢印を移動して下さい。このステップはページがウイルスおよびそれ以上のスコア低下ならスキャンが全域を通過して発生しないように必要です。

4. 設定が完了した変更を入れ、託して下さい。

このセットアップによって、ユーザが `www.example.com` に要求を送信するとき、WSAはこの要求に `Bypass.WBRS.id` を割り当てます。 `Bypass.WBRS.policy` が `Bypass.WBRS.id` に結合されるので、WSAは `Bypass.WBRS.policy` のために設定されるポリシーを適用します。このポリシーの WBRS 設定は -7.0 でブロックし始める従って要求は許可されず `configuredso` です。

注 カテゴリを使用し、URL カテゴリで許すために処理を設定する場合ウイルス対策 /Malware スキャンをバイパスします。その代り、監視するために処理を設定して下さい。