

セキュアWebアプライアンスでGoogle AIモードをブロックする

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定手順](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Google AIモードへのHTTPS要求をブロックするようにセキュアWebアプライアンス(HTTPS)を設定するために必要な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
- 基本的なネットワーキングおよびプロキシプロトコル
- SWAの復号化プロセス
- Regular Expressions] で以下を指定します。

次のツールをインストールしておくことを推奨します。

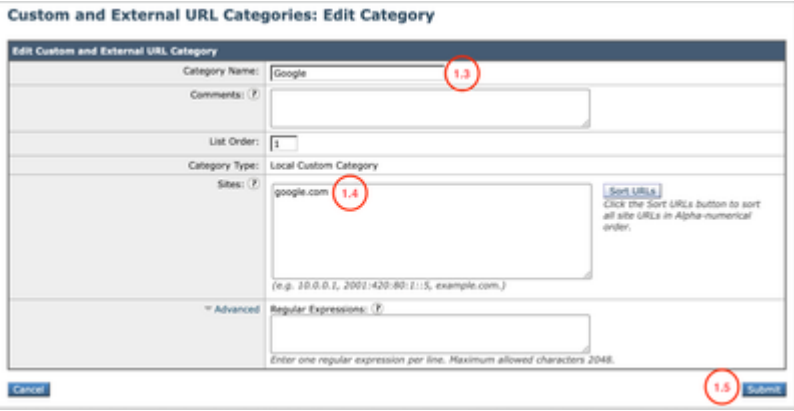
- 物理または仮想SWA
- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス

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たものです。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。

設定手順

<p>ステップ 1 : Google WebサイトのカスタムURLカテゴリを作成します。</p>	<p>ステップ 1.1 : GUIで、Web Security Managerに移動し、Custom and External URL Categoriesを選択します。</p> <p>ステップ 1.2 : Add Categoryをクリックして、新しいカスタムURLカテゴリを作成します。</p> <p>ステップ 1.3 : 新しいカテゴリの名前を入力します。</p> <p>ステップ 1.4 : サイトセクションで次のURLを定義します。</p> <p>google.com</p> <p>ステップ 1.5 : 変更を送信します。</p> 
<p>ステップ2:Google AIモード用のカスタムURLカテゴリを作成します。</p>	<p>ステップ 2.1 : GUIで、Web Security Managerに移動し、Custom and External URL Categoriesを選択します。</p> <p>ステップ 2.2 : Add Categoryをクリックして、新しいカスタムURLカテゴリを作成します。</p>

ステップ 2.3 : 新しいカテゴリの名前を入力します。

ステップ 2.4 : Regular Expressionsセクションで次のURLを定義します。

google\.com.*udm=50

ステップ 2.5 : 変更を送信します。



ヒント : カスタムURLカテゴリの設定方法の詳細については、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](#)

Custom and External URL Categories: Edit Category

ステップ 3 Googleのトラフィックを復号します。

ステップ 3.1 : GUIで、Web Security Managerに移動し、Decryption Policiesを選択します

ステップ 3.2 : Add Policyをクリックします。

ステップ 3.3 : 新しいポリシーの名前を入力します。

ステップ 3.4: (オプション) このポリシーを適用する必要があるIDプロファイルを選択します。

ステップ 3.5 : Policy Member Definitionセクションで、URL Categoriesリンクをクリックして、カスタムURLカ

カテゴリを追加します。

ステップ 3.6 : ステップ1で作成したURL カテゴリを選択します。

ステップ 3.7 : [Submit] をクリックします。

ステップ 3.8 : Decryption Policiesページで、新しいポリシーに対するURL Filteringからのリンクをクリックします。

ステップ 3.9 : カスタムURLカテゴリのアクションとして復号化を選択します。

ステップ 3.10 : [Submit] をクリックします。

Decryption Policies: URL Filtering: Decrypting Google Traffic

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Google	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

ステップ 4 Google AIモードトラフィックをブロックします。

ステップ 4.1 : GUIから、Web Security Managerに移動し、Access Policiesを選択します。

ステップ 4.2 : Add Policyをクリックします。

ステップ 4.3 : 新しいポリシーの名前を入力します。

Policy Name: Google AI Block (4.3)

Description: (Maximum allowed characters 256)

Insert Above Policy: 1 (getter server access policy)

Policy Expires: Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: 00:00

ステップ4.4 (オプション) このポリシーを適用する必要があるIDプロファイルを選択します。

ステップ 4.5 : ポリシーメンバー定義セクションで、URLカテゴリのリンクをクリックして、カスタムURLカテゴリを追加します。

ステップ 4.6 : ステップ2で作成したURL Categoryを選択します。

ステップ 4.7 : [Submit] をクリックします。

ステップ 4.8 : Access Policiesページで、新しいポリシーのURL Filtering からのリンクをクリックします。

ステップ 4.9 : カスタムURLカテゴリのアクションとしてBlockを選択します。

ステップ 4.10 : [Submit] をクリックします。

ステップ 4.11 : 変更を確定します。

確認

設定が完了すると、Google AIブロック用に作成したカスタムカテゴリによって検出され、Google AIトラフィックはブロックとしてアクセスログで処理されます。

<#root>

1779219170.427 101 10.184.103.26

TCP_DENIED_SSL/403

0 GET https://www.google.com:443/search?q=cisco+live+&sca_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo

BLOCK_CUSTOMCAT_12-Google_AI_Block

-ciscotest-NONE-NONE-NONE-NONE-NONE <"C_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_srch"

Google AIモードによる検索クエリの要求はブロックされ、このエンドユーザ通知が表示されます。



他のすべてのGoogleトラフィックは引き続き許可されます。

関連情報

[WSAでのカスタムURLカテゴリの定義](#)

[AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド](#)

[Secure Web Applianceでの復号化証明書の設定](#)

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。