Bloquer le mode AI de Google dans l'appareil Web sécurisé

Table des matières

Introduction

Ce document décrit les étapes nécessaires pour que l'appliance Web sécurisé soit configurée pour bloquer les requêtes HTTPS au mode AI de Google.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- administration SWA
- Protocoles réseau et proxy de base
- Processus de décryptage de la SWA
- Expressions régulières

Cisco recommande d'installer les outils suivants :

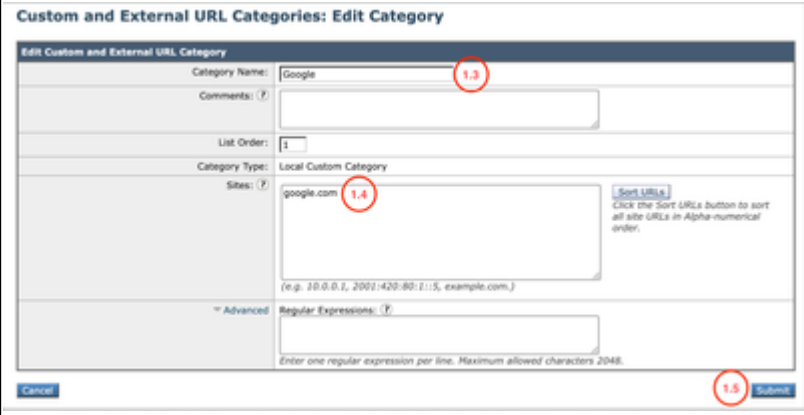
- SWA physique ou virtuel
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Étapes de configuration

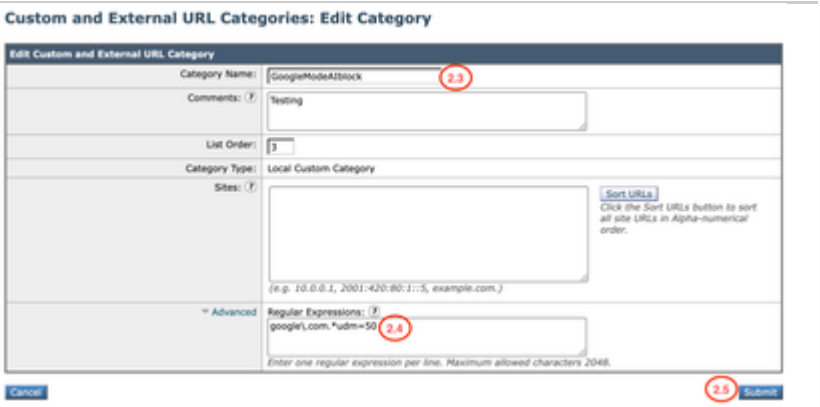
Étape 1 : création d'une catégorie d'URL personnalisée pour le site Web de Google	Étape 1.1. À partir de l’interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories. Étape 1.2. Cliquez sur Ajouter une catégorie pour créer une nouvelle catégorie d'URL personnalisée. Étape 1.3. Saisissez le nom de la nouvelle catégorie. Étape 1.4. Définissez ces URL dans la section Sites : `google.com` Étape 1.5. Soumettre les modifications 
Étape 2.Créez une catégorie d'URL personnalisée pour le mode AI de Google.	Étape 2.1. À partir de l’interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories. Étape 2.2. Cliquez sur Add Category pour créer une nouvelle catégorie d'URL personnalisée. Étape 2.3. Entrez le nom de la nouvelle catégorie.

<table>
<tr>
<td></td>
<td>Étape 2.4. Définissez ces URL dans la section Expressions régulières :

<code>google\.com.*udm=50</code>

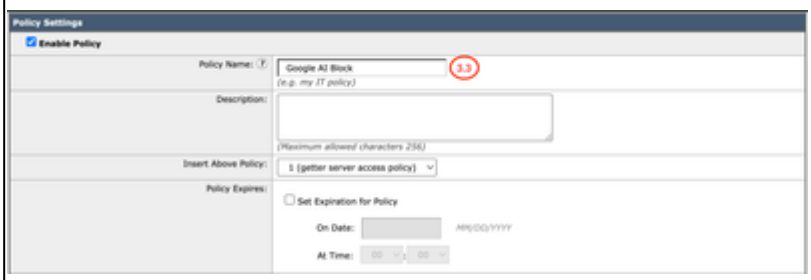
Étape 2.5. Soumettre les modifications

Conseil : Pour plus d'informations sur la façon de configurer des catégories d'URL personnalisées, consultez : Configurer des catégories d'URL personnalisées dans Appareil Web sécurisé - Cisco

 
</td>
</tr>
<tr>
<td>Étape 3. Déchiffrez le trafic pour Google.</td>
<td>Étape 3.1. À partir de l’interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Decryption Policies

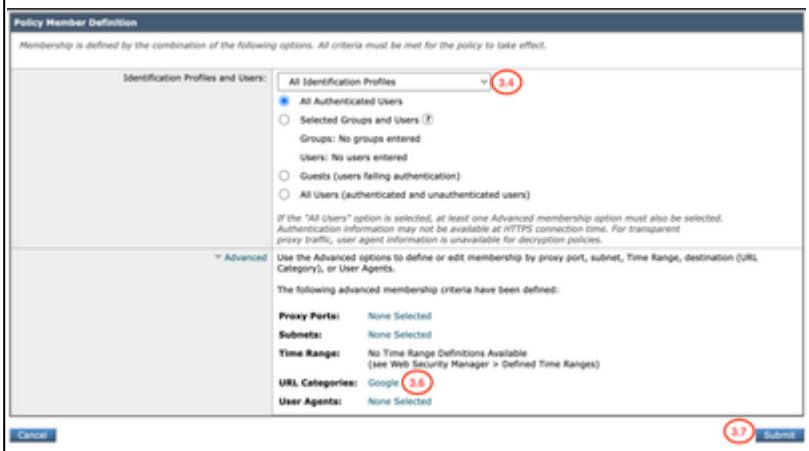
Étape 3.2. Cliquez sur Add Policy.

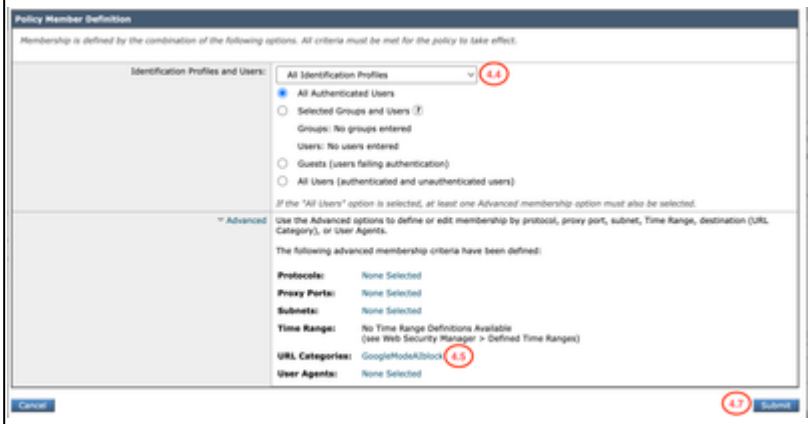
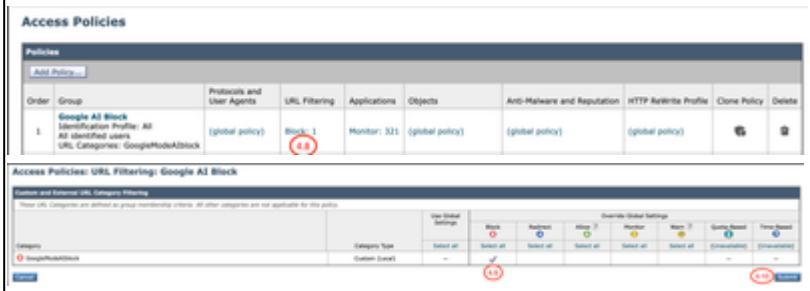
Étape 3.3. Entrez le nom de la nouvelle stratégie.

Étape 3.4. (Facultatif) Sélectionnez le profil d'identification auquel vous souhaitez que cette stratégie s'applique.

Étape 3.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour</td>
</tr>
</table>

	ajouter la catégorie d'URL personnalisée. Étape 3.6. Sélectionnez la catégorie d'URL créée à l'étape 1. Étape 3.7. Cliquez sur Submit.  Étape 3.8. Dans la page Decryption Policies, cliquez sur le lien de URL Filtering pour la nouvelle stratégie. Étape 3.9. Choisissez Decrypt comme action pour Custom URL Category. Étape 3.10. Cliquez sur Envoyer. 
Étape 4 : blocage du trafic en mode AI de Google	Étape 4.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Access Policies. Étape 4.2. Cliquez sur Add Policy. Étape 4.3. Entrez le nom de la nouvelle stratégie. 

	Étape 4.4. (Facultatif) Sélectionnez le profil d'identification auquel vous souhaitez que cette stratégie s'applique. Étape 4.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée. Étape 4.6. Sélectionnez la catégorie d'URL créée à l'étape 2. Étape 4.7. Cliquez sur Submit.  Étape 4.8. Dans la page Stratégies d'accès, cliquez sur le lien du filtrage d'URL pour la nouvelle stratégie. Étape 4.9. Choisissez Block comme action pour Custom URL Category. Étape 4.10. Cliquez sur Submit.  Étape 4.11. Valider les modifications

Vérifier

Lorsque les paramètres de configuration sont terminés, le trafic Google AI est traité sur les journaux d'accès comme Bloquer, car il est détecté par la catégorie personnalisée que nous avons créée pour Google AI Block.

<#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_GooO",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_srch"

Une requête de recherche en mode Google AI est bloquée et affiche cette notification de l'utilisateur final.

Tout autre trafic Google continue d'être autorisé.

Informations connexes

Définir des catégories d'URL personnalisées dans WSA

Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance

Configurer le certificat de déchiffrement dans l'appareil Web sécurisé

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.