Bloquer l'accès aux comptes clients Google dans le SWA

Table des matières

Introduction

Ce document décrit le processus de blocage de l'accès à Google Workspace ou à Google Consumer Accounts dans Secure Web Appliance (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface graphique utilisateur (GUI) de SWA
- Accès administratif au 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.

Configurer

<table>
<tr>
<td>Étape 1.Créez une catégorie d'URL personnalisée pour les sites Google.</td>
<td>Étape 1.1. Dans l'interface graphique utilisateur, accédez à Web Security Manager et sélectionnez Custom and External URL Categories.

Étape 1.2. Cliquez sur Add Category (Ajouter une catégorie) pour créer une nouvelle catégorie d'URL personnalisée.

Étape 1.3. Entrez le nom de la nouvelle catégorie.

Étape 1.4. Définissez ces URL dans la section Sites :

<code>.google.com</code>

Étape 1.5. Envoyez les modifications.

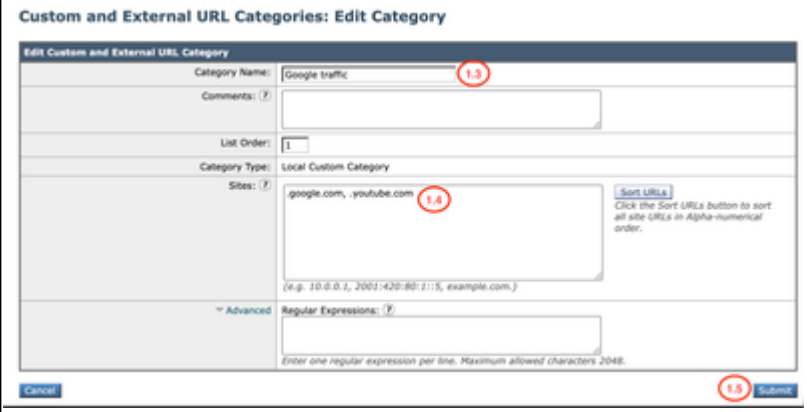
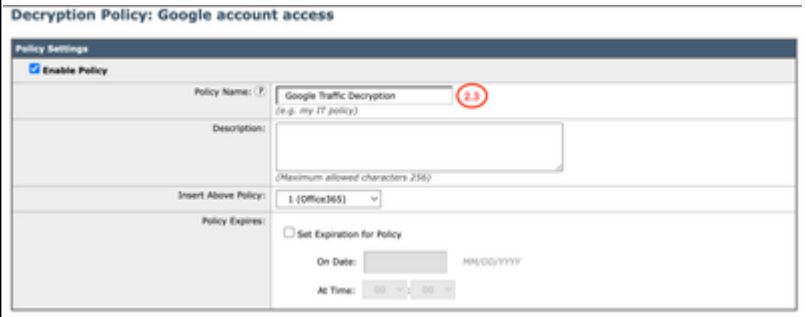
 

Image - Catégorie d'URL personnalisée

Conseil : Pour plus d'informations sur la configuration des catégories d'URL personnalisées, veuillez consulter : Configurer des catégories d'URL personnalisées dans l'appliance Web sécurisée.</td>
</tr>
<tr>
<td>Étape 2 : décodage du trafic</td>
<td>Étape 2.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Decryption Policies.</td>
</tr>
</table>

Étape 2.2. Cliquez sur Add Policy.

Étape 2.3. EnterName pour la nouvelle stratégie



Étape 2.4. Sélectionnez le profil d'identification auquel cette stratégie doit s'appliquer.

Conseil : Si vous avez ignoré les authentifications pour les URL Microsoft et que vous configurez cette stratégie pour Tous les utilisateurs, choisissez : Tous les profils d'identification > Tous les utilisateurs.

Étape 2.5. Dans la section Définition de membre de stratégie, cliquez sur les liens de catégories d'URL pour ajouter la catégorie d'URL personnalisée.

Étape 2.6.Sélectionnez la catégorie d'URL créée à l'étape 1.

Étape 2.7.Cliquez sur Envoyer.

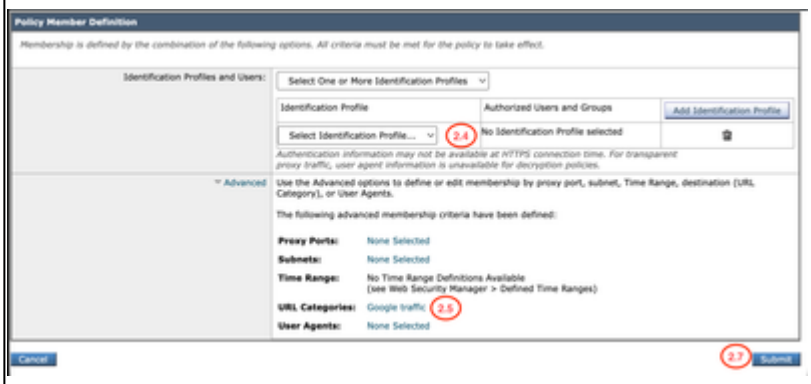
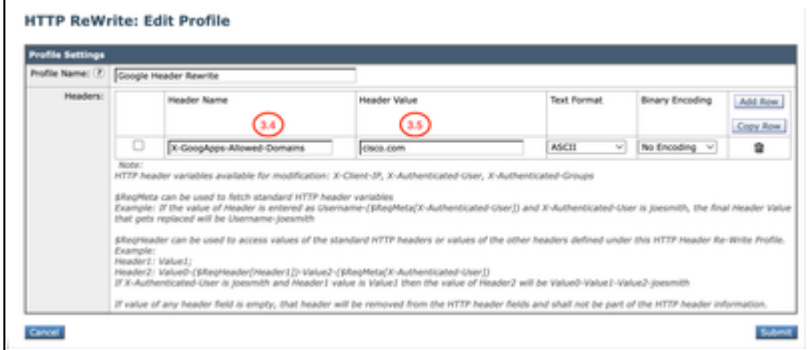
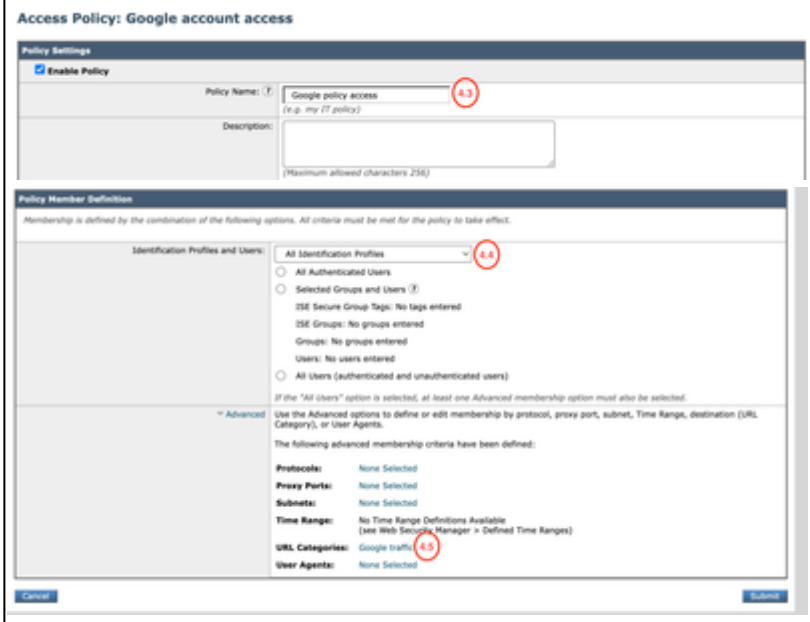
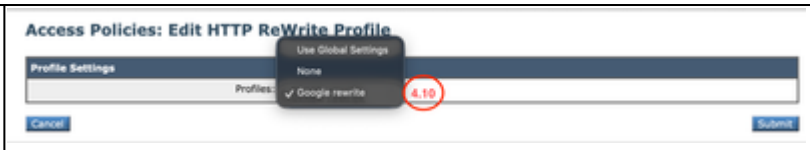


Image - Configurer la stratégie de déchiffrement

Étape 2.8. InDecryption Policies page, cliquez sur le lien fromURL Filtering pour la nouvelle stratégie.

	Image - Modifier l'action de filtrage URL Étape 2.9. Choisir Décrypter comme action pour Catégorie d'URL personnalisée. Étape 2.10.Cliquez sur Envoyer.  Image - Déchiffrer la catégorie d'URL personnalisée.
Étape 3 : création du profil de réécriture HTTP	Étape 3.1.Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnezHTTP ReWrite Profiles. Étape 3.2. Cliquez sur Ajouter un profil. Étape 3.3. Entrez un nom pour le nouveau profil. Étape 3.4. Utiliser X-GoogApps-Allowed-Domains pour le premier nom d'en-tête. Étape 3.5. Pour le paramètre Restrict-Access-To-Tenants, utilisez une valeur de domaine de liste de locataires autorisés, qui doit être une liste séparée par des virgules des locataires auxquels les utilisateurs sont autorisés à accéder. Étape 3.9.Cliquez sur Envoyer.  Image - Ajouter un profil de réécriture HTTP

Étape 4 : création d'une stratégie d'accès	Étape 4.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Access Policies. Étape 4.2. Cliquez sur Add Policy. Étape 4.3. EnterName pour la nouvelle stratégie. Étape 4.4. (Facultatif) Sélectionnez le profil d'identification auquel cette stratégie doit s'appliquer. Étape 4.5.Dans la section Définition de membre de stratégie, cliquez sur Liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée. Étape 4.6.Sélectionnez la catégorie d'URL créée à l'étape 1. Étape 4.7. Cliquez sur Envoyer.  Image - Créer une stratégie d'accès Étape 4.8.Dans la page Stratégies d'accès, assurez-vous que l'action du filtrage d'URL est définie sur Surveiller. Étape 4.9.Cliquez sur le lien dans HTTP ReWrite Profile pour ajouter le profil d'en-tête HTTP à cette stratégie.  Image - Propriétés de la stratégie d'accès Étape 4.10. Choisissez les profils de réécriture HTTP, créés à l'étape [3].

	 Image - Ajouter un profil de réécriture HTTP Étape 4.11. Cliquez sur Envoyer. Étape 4.12. CommitChanges

Rapports et journaux

Journaux

Vous pouvez ajouter des champs personnalisés aux journaux d'accès ou aux journaux W3C pour afficher le nom du profil de réécriture de l'en-tête HTTP.

Spécificateur de format dans les journaux d'accès	Champ Log dans les journaux W3C	Description
%]	x-http-rewrite-profile-name	Nom du profil de réécriture d'en-tête HTTP.

Vous pouvez générer un rapport de suivi Web pour afficher les rapports du trafic en fonction du nom de la stratégie d'accès.

Pour générer les rapports, procédez comme suit :

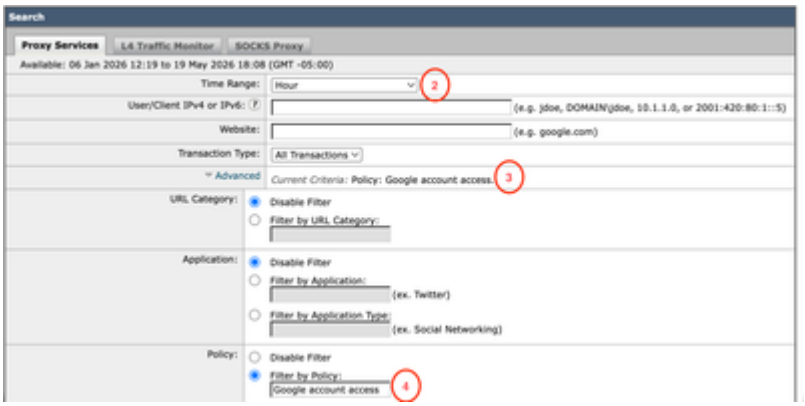
Étape 1. Dans l’interface utilisateur graphique, sélectionnezGénération de rapports et sélectionnezSuivi Web.

Étape 2. Choisissez la plage horaire souhaitée.

Étape 3. Cliquez sur le lien Avancé pour rechercher des transactions à l'aide de critères avancés.

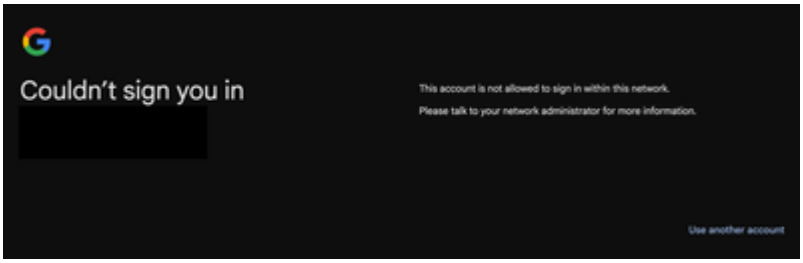
Étape 4. Dans la section Stratégie, sélectionnez Filtrer par stratégie et tapez le nom de la stratégie d'accès qui a été créée précédemment.

Étape 5. Cliquez sur Rechercher pour consulter le rapport.



Vérifier

Lorsque la configuration de restriction de domaine Google est terminée, l'utilisateur peut uniquement accéder aux comptes qui se trouvent sous le domaine configuré sur le profil de réécriture d'en-tête à l'étape 3. Si l'utilisateur essaie d'accéder à un compte sur un autre domaine, ou un autre compte personnel, Google, l'accès est restreint avec cette notification :



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]

[Réécriture de l'en-tête HTTP WSA]

[Bloquer l'accès aux comptes clients (documentation Google)]

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.