Définir des catégories d'URL personnalisées dans WSA

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Autoriser les URL
    - Créer une nouvelle URL personnalisée
    - Modifier la stratégie d'accès globale
  - Bloquer les URL
    - Créer une nouvelle URL personnalisée
    - Modifier la stratégie d'accès globale

Introduction

Ce document décrit comment vous pouvez définir des catégories d'URL personnalisées dans l'appliance de sécurité Web (WSA).

Contribution de Shikha Grover et sous la direction de Yeraldin Sanchez, Ingénieurs du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Niveau débutant de compréhension de l'appliance de sécurité Web Cisco

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.

Informations générales

La catégorie à laquelle appartient une URL est déterminée par une base de données de catégories de filtrage. L'appliance de sécurité Web collecte des informations et gère une base de données distincte pour chaque moteur de filtrage d'URL. Les bases de données de catégories de filtrage reçoivent régulièrement des mises à jour du serveur de mise à jour Cisco et sont gérées par Cisco TALOS. Talos, le groupe Cisco Security Intelligence and Research, suit en permanence un large éventail d'attributs pour évaluer les conclusions relatives à un hôte donné.

Il peut arriver que vous souhaitiez classer une adresse URL/domaine/IP différemment et que vous ayez une classification personnalisée locale à votre boîte. Vous pouvez y parvenir avec des catégories d'URL personnalisées.

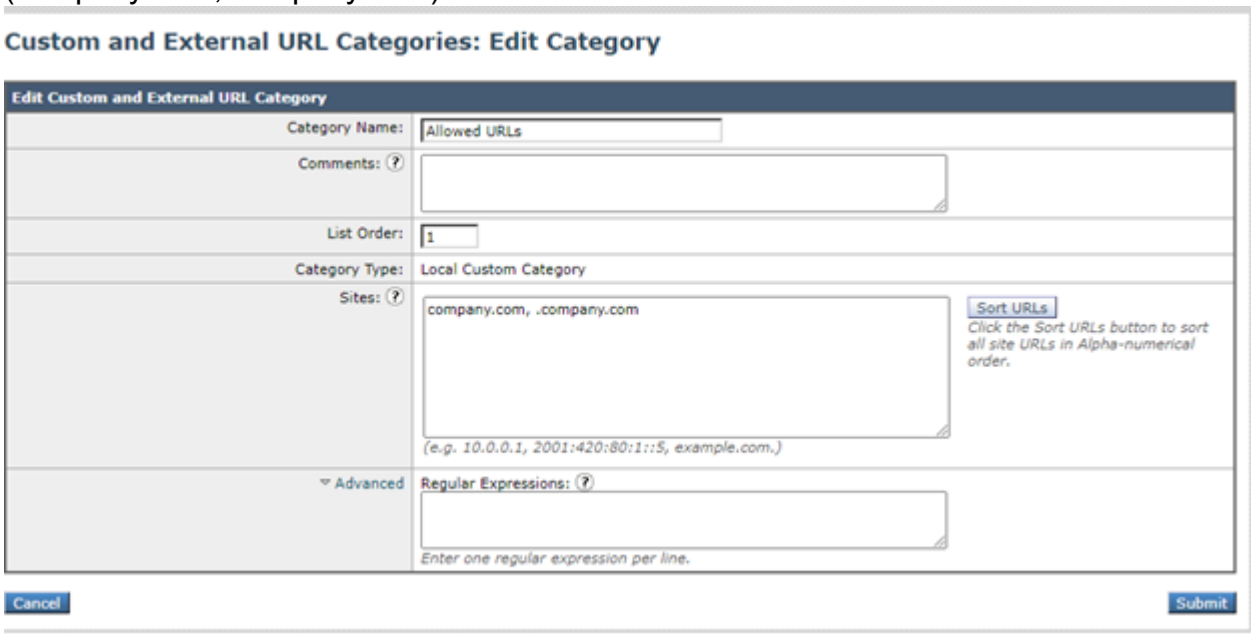
Lorsque le moteur de filtrage d'URL fait correspondre une catégorie d'URL à l'URL d'une demande client, il évalue d'abord l'URL par rapport aux catégories d'URL personnalisées incluses dans le groupe de stratégies. Si l'URL de la demande ne correspond pas à une catégorie personnalisée incluse, le moteur de filtrage d'URL la compare aux catégories d'URL prédéfinies.

Configurer

Autoriser les URL

Si vous faites confiance au site Web, vous pouvez l'autoriser avec le processus suivant.

Créer une nouvelle URL personnalisée

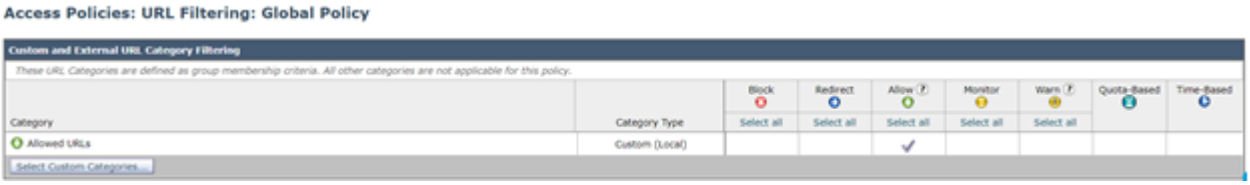
1. Créez une nouvelle catégorie d'URL personnalisée, accédez à GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name : URL autorisées.
2. Ajoutez les sites que vous souhaitez contrôler dans la section Sites (company.com,.company.com).
3. 

4. Notez que « domain.com » correspond uniquement à « domain.com », et non à www.domain.com ou à « host.domain.com ». Afin de permettre un site et tous les sous-domaines, il aura besoin de deux entrées sous la section « sites » : « . domain.com,

domain.com ».
5. Cliquez sur Submit.

Modifier la stratégie d'accès globale

1. Ouvrez Gestionnaire de sécurité Web > Stratégies d'accès > Stratégie globale > Filtrage des URL.
2. Cliquez sur Sélectionner des catégories personnalisées.
3. Cliquez sur la flèche de la liste déroulante URL autorisées, choisissez Inclure dans la stratégie, puis cliquez sur Appliquer.
4. Cochez la case Allow (Autoriser).
5. Cliquez sur Submit and Commit Changes.

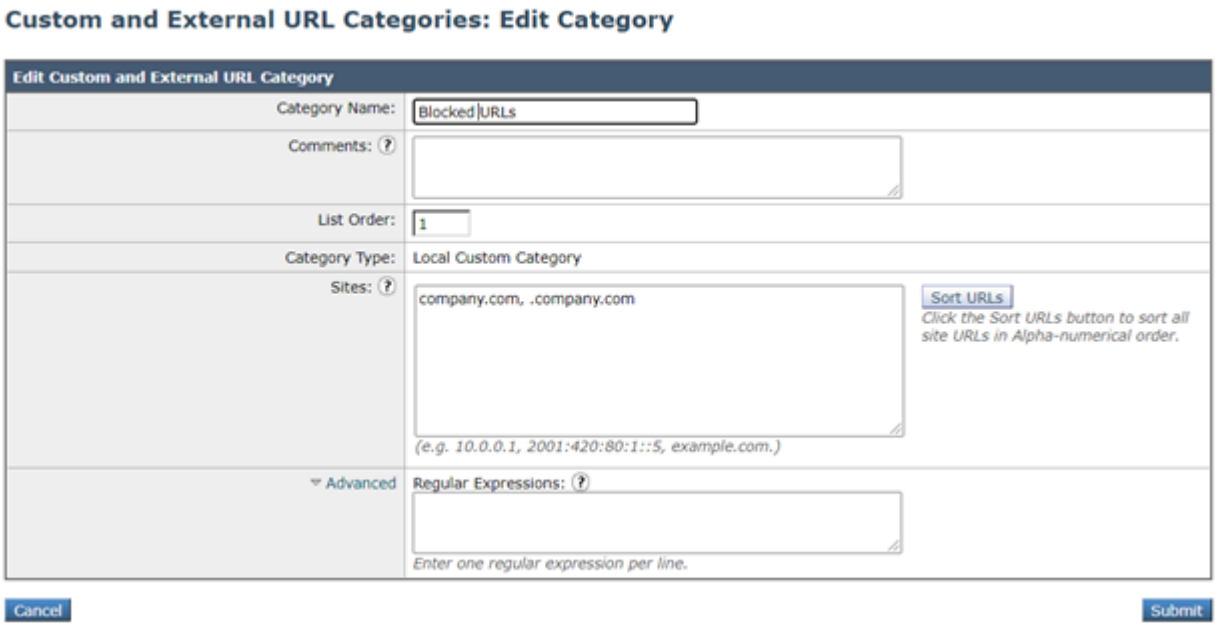


Bloquer les URL

Si vous ne faites pas confiance au site Web, vous pouvez le bloquer en procédant comme suit.

Créer une nouvelle URL personnalisée

1. Créez une nouvelle catégorie d'URL personnalisée, accédez à GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name : URL bloquées.
2. Ajoutez les sites à contrôler dans la section Sites (company.com, .company.com).



3. Notez que « domain.com » correspond uniquement à « domain.com », et non à www.domain.com ou à « host.domain.com ». Afin de bloquer un site et tous les sous-domaines, il aura besoin de deux entrées sous la section « sites » : « . domain.com, domain.com ».

4. Cliquez sur Submit.

Modifier la stratégie d'accès globale

1. Ouvrez Gestionnaire de sécurité Web > Stratégies d'accès > Stratégie globale > Filtrage des URL.
2. Cliquez sur Sélectionner des catégories personnalisées...
3. Cliquez sur la flèche de la liste déroulante URL bloquées, sélectionnez Inclure dans la stratégie, puis cliquez sur Appliquer.
4. Cochez la case Block (Bloquer).
5. Cliquez sur Submit and Commit Changes.



Remarque : les modifications ci-dessus peuvent être apportées à n'importe quelle stratégie d'accès et pas seulement à la stratégie globale. La même procédure peut être appliquée aux stratégies de déchiffrement.

Consultez ce guide pour un exemple d'utilisation largement déployé.

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.