# Définir des catégories d'URL personnalisées dans WSA

## Contenu

Introduction

Conditions préalables

Conditions requises

Components Used

Informations générales

Configuration

Autoriser les URL

Créer une URL personnalisée

Modifier la stratégie d'accès globale

Bloquer les URL

Créer une 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).

Contribué par Shikha Grover et édité par Yeraldin Sanchez, Ingénieurs du TAC Cisco.

# Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

• Compréhension de niveau débutant de l'appliance de sécurité Web Cisco

## **Components Used**

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 dans laquelle se trouve 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 des catégories de filtrage reçoivent régulièrement des mises à jour du serveur de mise à jour Cisco et sont gérées par Cisco TALOS. Talos, le Security Intelligence and Research Group de Cisco, suit constamment un large éventail d'attributs pour évaluer les conclusions relatives à un hôte donné.

Il peut y avoir des situations où vous voulez classer une adresse URL/domaine/IP différemment et avoir 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 dans 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.

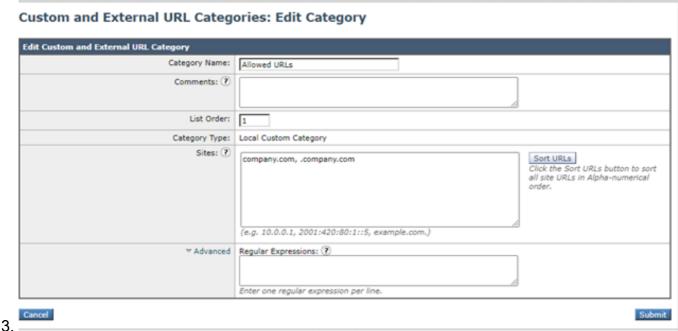
# Configuration

#### Autoriser les URL

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

### Créer une URL personnalisée

- Créez une nouvelle catégorie d'URL personnalisée, accédez à GUI > Gestionnaire de sécurité Web > Catégories d'URL personnalisées > Ajouter un nom de catégorie personnalisé : URL autorisées.
- 2. Ajoutez les sites que vous souhaitez contrôler dans la section Sites (company.com..company.com).



- 4. Veuillez noter que " domaine.com " ne correspond qu'à " domaine.com ", et non <a href="https://www.domain.com">www.domain.com</a> ou " host.domain.com ". Afin d'autoriser un site et tous les sous-domaines, il aura besoin de deux entrées dans la section " sites " : ". domain.com, domain.com ".
- 5. Cliquez sur Submit.

#### Modifier la stratégie d'accès globale

- 1. Ouvrez Web Security Manager > Access Policies > Global Policy > URL Filtering.
- 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 Autoriser.
- 5. Cliquez sur Soumettre et valider les modifications.

Access Policies: URL Filtering: Global Policy



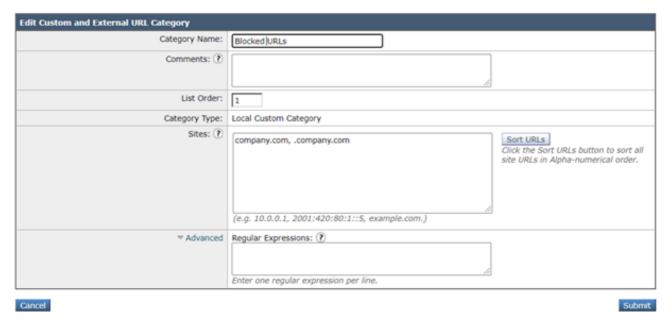
## Bloquer les URL

Si vous ne faites pas confiance au site Web, vous pouvez le bloquer en suivant la procédure suivante.

#### Créer une URL personnalisée

- Créez une nouvelle catégorie d'URL personnalisée, accédez à GUI > Gestionnaire de sécurité Web > Catégories d'URL personnalisées > Ajouter un nom de catégorie personnalisé : URL bloquées.
- 2. Ajoutez les sites que vous souhaitez contrôler dans la section Sites (company.com, .company.com).

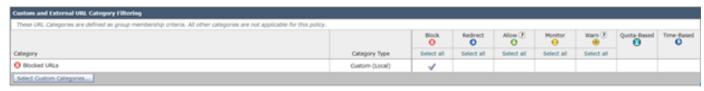
**Custom and External URL Categories: Edit Category** 



- 3. Veuillez noter que " domaine.com " ne correspond qu'à " domaine.com ", et non www.domain.com ou " host.domain.com ". Afin de bloquer un site et tous les sous-domaines, il aura besoin de deux entrées dans la section " sites " : ". domain.com, domain.com ".
- 4. Cliquez sur Submit.

- 1. Ouvrez Web Security Manager > Access Policies > Global Policy > URL Filtering.
- 2. Cliquez sur Sélectionner des catégories personnalisées....
- 3. Cliquez sur la flèche de la liste déroulante **URL bloquées**, choisissez Inclure dans la stratégie et cliquez sur **Appliquer**.
- 4. Cochez la case Bloquer.
- 5. Cliquez sur Soumettre et valider les modifications.

Access Policies: URL Filtering: Global Policy



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

Veuillez consulter ce guide pour un cas d'utilisation largement répandu.