

Dépannage et vérification de la catégorie d'URL dans CSF

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Produits associés](#)

[Informations générales](#)

[Architecture](#)

[Étape 1: Rechercher la catégorie d'URL dans FMC](#)

[Étape 2: Vérifier les paramètres d'intégration du filtrage URL](#)

[Étape 3: Confirmez la catégorie d'URL sur le périphérique à l'aide de la trace de support système](#)

[Étape 4: Résoudre le numéro de catégorie en un nom de catégorie](#)

[Vérifier](#)

[Bouton Litige](#)

[Dépannage](#)

Introduction

Ce document décrit comment vérifier les attributions de catégorie d'URL sur Secure Firewall et FMC pour s'assurer que le périphérique utilise la même classification d'URL.

Conditions préalables

Vous devez avoir activé la licence de filtrage d'URL pour le périphérique, l'intégration des services cloud dans un état sain et une stratégie de contrôle d'accès qui inclut le filtrage d'URL et a été déployée après la configuration de la condition d'URL.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Filtrage des URL et recherche de catégories dans Firepower Management Center (FMC)
- Inspection du trafic Cisco Secure Firewall (CSF) et évaluation des politiques
- Classement des URL et comportement de réputation, basé sur Talos à partir de CSF version 6.5

Composants utilisés

Ce document décrit les fonctionnalités disponibles dans Cisco Secure Firewall et FMC versions 6.5 et ultérieures. Les exemples de ce guide utilisent la version 7.6.5.

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.

Produits associés

Ce document peut également être utilisé avec les produits et versions suivants :

- Centre de gestion du pare-feu sécurisé (FMC)
- Cisco Secure Firewall (CSF)
- Filtrage des URL et intégrations de services cloud

Informations générales

Le filtrage d'URL repose sur une base de données de catégories évaluée lors de l'inspection du trafic. Le FMC stocke les informations de catégorie d'URL pour une destination, et le périphérique effectue une recherche d'exécution lorsque le trafic est inspecté. En cas de non-correspondance entre le FMC, le périphérique ou la base de données cloud, les résultats de la stratégie peuvent sembler incohérents, même si la stratégie de contrôle d'accès est correctement configurée.

Une partie importante de la vérification consiste à confirmer que l'attribution de catégorie d'URL est cohérente à travers le FMC et le périphérique. La recherche de catégorie d'URL est influencée par les paramètres d'intégration des services cloud et le cache de périphérique. Si le paramètre d'actualisation du cache est désactivé ou si la durée de vie de l'entrée est trop longue, les données de catégorie périmées peuvent rester utilisées une fois que Talos a mis à jour la classification.

Architecture

Lorsque le filtrage des URL est activé, le périphérique vérifie d'abord le cache d'URL local. Si la catégorie n'est pas déjà présente dans le cache, le périphérique peut interroger la base de données locale ou le cloud Cisco. Le périphérique utilise sa base de données d'URL locale et son cache de recherche pendant l'inspection, et beakerd communique avec Talos pour télécharger et mettre à jour les données de filtrage d'URL. Sur les périphériques gérés par FMC, beakerd s'exécute sur FMC et est en état d'attente sur le CSF. Si le CSF est géré localement, le processus s'exécute sur le périphérique lui-même.

Talos envoie des packages de base de données complets dans plusieurs tailles, stockés sous `/var/sf/cloud_download/cisco`.

Voici quelques exemples de ce à quoi peuvent ressembler les fichiers de base de données de Talos :

- `cisco_uridb_large_1541554243` (500 Mo)
- `cisco_uridb_medium_1541553645` (125 Mo)
- `cisco_uridb_small_1541553061` (33 Mo)



Remarque : Les fichiers de base de données commencent par `cisco_uridb`, puis la taille est indiquée (petite, moyenne ou grande). Les tailles peuvent varier en fonction du matériel utilisé.

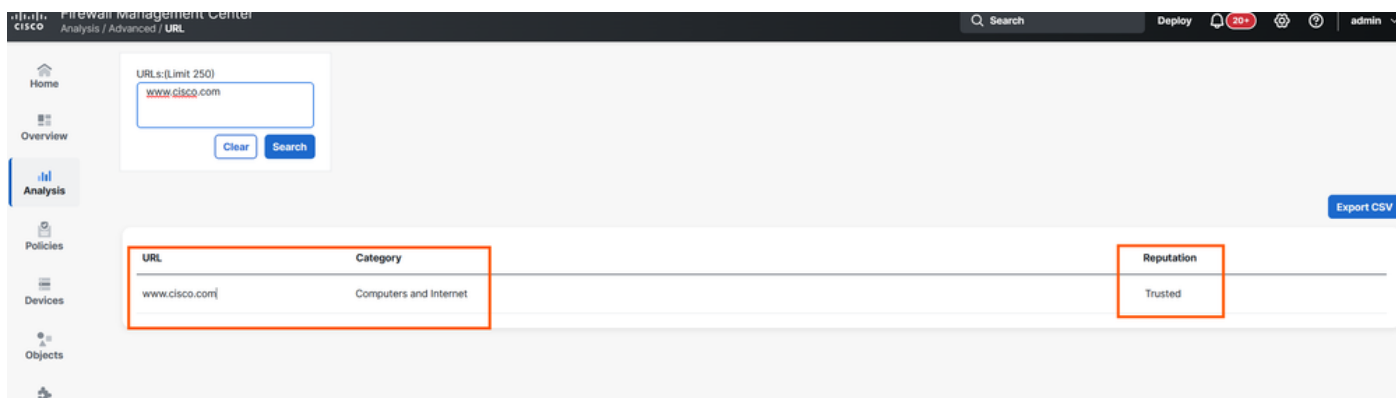
Étape 1: Rechercher la catégorie d'URL dans FMC

Le FMC gère une base de données d'URL locale qui mappe les destinations d'URL aux catégories qui leur sont attribuées. Il s'agit de la première étape recommandée lors de la validation de la classification d'une URL.

Accédez à l'emplacement `Analysis > Advanced > URL` dans FMC.

Saisissez l'URL que vous souhaitez rechercher et vérifiez la catégorie qui lui est affectée.

Dans l'exemple ci-dessous, www.cisco.com est répertorié dans la catégorie Ordinateurs et Internet.



Étape 2: Vérifier les paramètres d'intégration du filtrage URL

Les paramètres d'intégration du filtrage des URL déterminent où le FMC et le périphérique CSF alimentent leur base de données de catégories d'URL. Chaque périphérique gère sa propre base de données locale pour la recherche d'URL et peut interroger le cloud Cisco pour obtenir des informations supplémentaires ou mises à jour sur les URL.

Accédez à **Integration > Other Integrations > Cloud Services** dans FMC pour passer en revue ces paramètres.

URL Filtering

Last URL Filtering Update: 2026-08-26 10:28:52 [Update Now](#)

☒ Enable Automatic Updates

URL Query Source

☐ Local Database Only

☒ Local Database and Cisco Cloud

☐ Cisco Cloud Only

Cached URLs Expire

After 2 hours

[Dispute URL categories and reputations](#)

Save

Vérifiez que l'intégration est saine et que le cache de recherche d'URL est configuré pour être actualisé en fonction de la durée de stratégie attendue.



Mise en garde : Le cache de recherche d'URL peut conserver les résultats de catégorie et de réputation précédemment récupérés. Si l'expiration du cache est désactivée ou configurée avec une longue durée de vie, le périphérique peut continuer à utiliser les informations mises en cache après que Talos a mis à jour la classification, ce qui peut entraîner une différence temporaire entre le résultat du périphérique et la recherche FMC ou Talos actuelle.

Étape 3: Confirmez la catégorie d'URL sur le périphérique à l'aide de la trace de support système

Pour vérifier que le périphérique CSF catégorise l'URL de la même manière que le FMC, exécutez

une trace de support système à partir de l'interface de ligne de commande du périphérique. Cette section montre comment le moteur d'inspection Snort évalue le trafic et quelle catégorie d'URL est retournée lorsque la connexion est inspectée.

Dans l'interface de ligne de commande FTD, entrez la commande `system support trace` et répondez aux invites interactives :

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 173.37.145.84
Please specify a server port: 443
```



Remarque : Dans cet exemple, 173.37.145.84 est l'adresse IP de www.cisco.com. Utilisez l'adresse IP de destination qui correspond à l'URL que vous recherchez.

Exemple de rapport :

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1: returned from url lookup, url_info is 90 20
```

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1 URL lookup for www.cisco.com/ found rep 90, c
```

Dans cette sortie, l'URL renvoie l'ID de catégorie 2003. L'étape suivante explique comment convertir cette valeur numérique en nom de catégorie correspondant.

Étape 4: Résoudre le numéro de catégorie en un nom de catégorie

La recherche de catégorie URL sur le périphérique renvoie un ID de catégorie numérique. Pour mapper ce numéro à un nom de catégorie lisible par l'utilisateur, ouvrez le fichier `aup_categories.json` sur le périphérique.

Accédez au répertoire `/var/sf/cloud_download/` sur le CSF en mode expert. Assurez-vous que vous êtes en mode utilisateur racine.

Ouvrez le fichier de définitions de catégorie :

```
root@firepower:/var/sf/cloud_download# less aup_categories.json
```

Recherchez l'ID de catégorie renvoyé dans la sortie de trace. Exemple d'entrée pour la catégorie 2003 :

```
{
  "id": 2003,
  "uuid": "abba9b63-bb10-4729-b901-2e2aa0f02003",
  "mnemonic": "comp",
  "name": "Computers and Internet",
  "type": "aup_cats",
  "state": "active"
}
```



Remarque : Les numéros d'ID de catégorie sont cohérents sur tous les périphériques CSF. Le même ID numérique correspond au même nom de catégorie sur chaque périphérique CSF.

Vérifier

Utilisez le résultat des étapes 1 à 4 pour confirmer que l'attribution de catégorie d'URL est cohérente entre la base de données FMC et le moteur Snort sur le périphérique.

Dans cet exemple :

- La base de données FMC répertorie www.cisco.com comme Ordinateurs et Internet.
- L'interface de ligne de commande du périphérique renvoie la catégorie ID 2003, qui correspond à Ordinateurs et Internet.

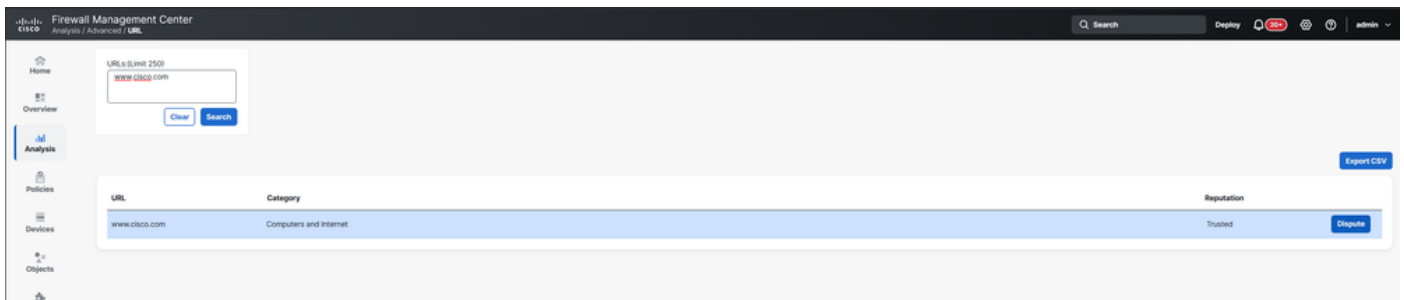
Les deux sources sont d'accord, ce qui confirme que la stratégie de filtrage d'URL appliquée est cohérente pour cette URL.

Bouton Litige

Si vous pensez qu'une URL a été classée dans une catégorie incorrecte, vous pouvez soumettre un litige à Talos.

Accédez à Analysis > Advanced > URL dans FMC :

Saisissez l'URL, cliquez sur Rechercher, puis passez le curseur sur l'entrée d'URL et sélectionnez Litige.



La page Conflit Talos s'ouvre, de sorte que la classification puisse être révisée et corrigée par la source appropriée.

Dépannage

Si la classification ne correspond pas aux attentes, passez en revue les éléments suivants :

- Vérifiez que la licence de filtrage d'URL est activée et attribuée au périphérique.
- Vérifiez l'intégrité des services cloud et la connexion à Talos.
- Vérifiez les paramètres de mise à jour du cache et du cache du périphérique pour vous assurer que les entrées périmées ne sont pas réutilisées.
- Vérifiez si le processus en cascade est en cours d'exécution sur le FMC pour les périphériques gérés par FMC.

Pour les périphériques gérés par FMC, exécutez cette commande en mode expert FMC pour confirmer que le processus est actif :

```
pmtool status | grep beakerd
```



Remarque : Si vous exécutez cette commande dans un pare-feu sécurisé qui est géré par FMC, le processus peut être vu dans un état d'attente. Si le pare-feu sécurisé est géré

localement, le processus est considéré comme étant en cours d'exécution.

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.