Résolution des problèmes de filtrage des URL sur un système FireSIGHT

Contenu

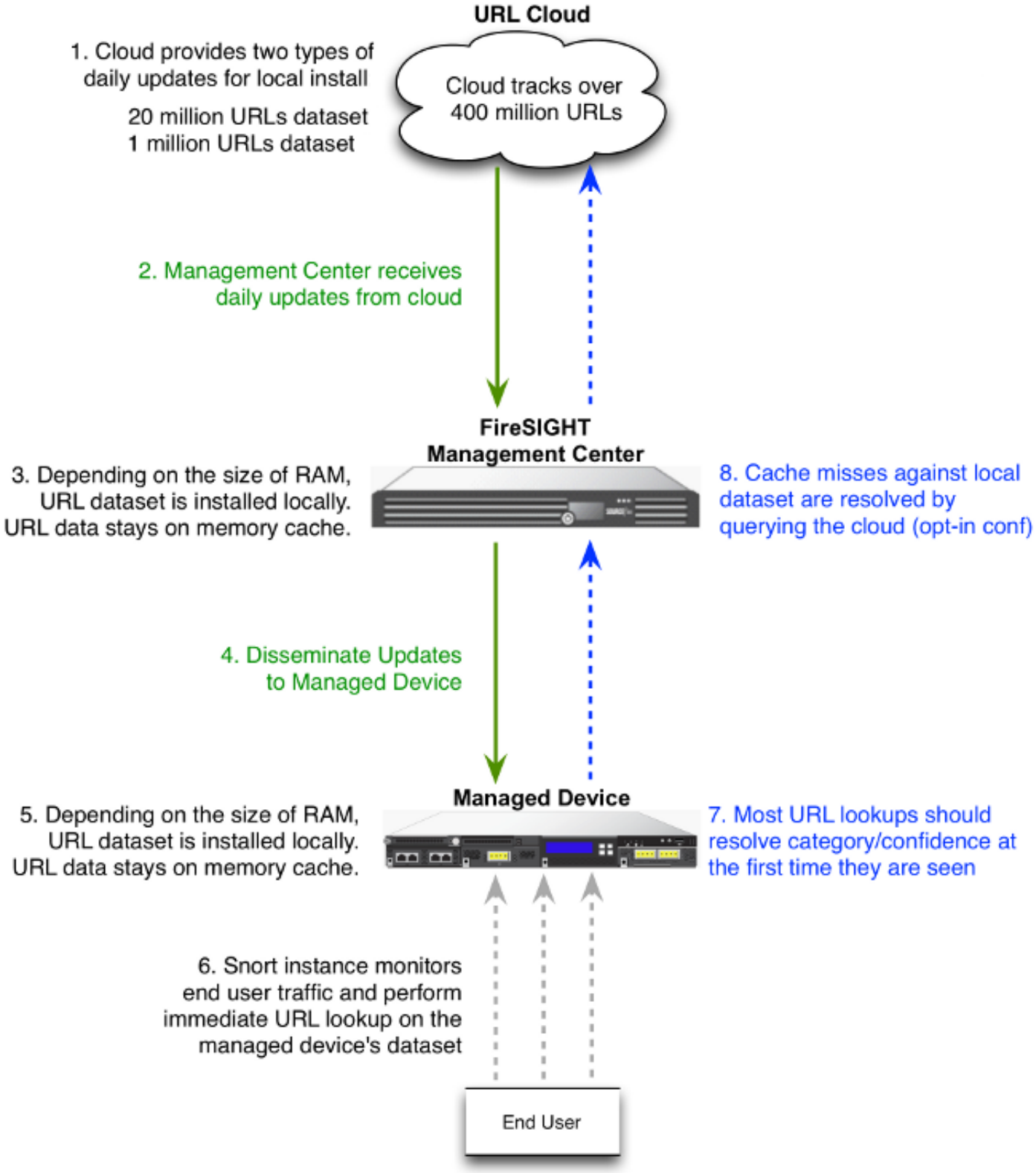
Introduction

Ce document décrit les problèmes courants liés au filtrage des URL. La fonction de filtrage des URL de FireSIGHT Management Center catégorise le trafic des hôtes surveillés et vous permet d'écrire une condition dans une règle de contrôle d'accès basée sur la réputation.

Processus de recherche de filtrage URL

Afin d'accélérer le processus de recherche d'URL, le filtrage d'URL fournit un jeu de données installé localement sur un système Firepower. Selon la quantité de mémoire (RAM) disponible sur un appareil, il existe deux types de jeux de données :

Type de dataset	Besoins en mémoire	
	Sur la version 5.3	Sur la version 5.4 ou ultérieure
20 millions d'URL	>2 Go	>3,4 Go
1 million d'URL Dataset	<= 2 Go	<= 3,4 Go



Problèmes de connectivité cloud

Étape 1 : Vérifier les licences

La licence est-elle installée ?

Vous pouvez ajouter des conditions d'URL basées sur la catégorie et la réputation aux règles de contrôle d'accès sans licence de filtrage d'URL. Toutefois, vous ne pouvez pas appliquer la stratégie de contrôle d'accès tant que vous n'avez pas d'abord ajouté une licence de filtrage

d'URL à FireSIGHT Management Center, puis l'avez activée sur les périphériques ciblés par la stratégie.

La licence a-t-elle expiré ?

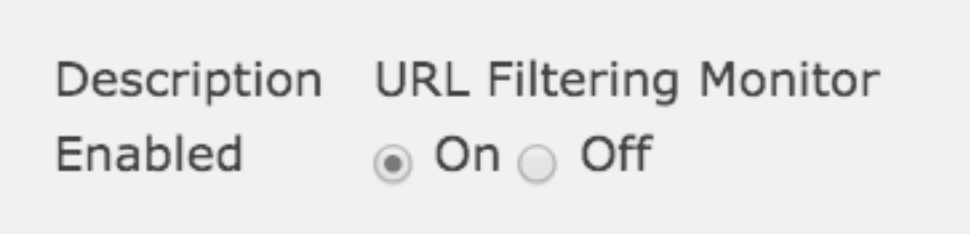
Si une licence de filtrage d'URL expire, les règles de contrôle d'accès avec des conditions d'URL basées sur la catégorie et la réputation arrêtent le filtrage des URL et FireSIGHT Management Center ne contacte plus le service cloud.

> **Astuce** : Lisez l'exemple de configuration du filtrage d'URL sur un système FireSIGHT afin d'apprendre comment activer la fonctionnalité de filtrage d'URL sur un système FireSIGHT et appliquer la licence de filtrage d'URL sur un périphérique géré.

Étape 2 : Vérifier les alertes de santé

Le module URL Filtering Monitor assure le suivi des communications entre FireSIGHT Management Center et le cloud Cisco, où le système obtient ses données de filtrage d'URL (catégorie et réputation) pour les URL fréquemment visitées. Le module de surveillance du filtrage des URL assure également le suivi des communications entre FireSIGHT Management Center et tout périphérique géré sur lequel vous avez activé le filtrage des URL.

Afin d'activer le module Moniteur de filtrage d'URL, allez à la page **Configuration de la stratégie d'intégrité**, choisissez **Moniteur de filtrage d'URL**. Cliquez sur la case d'option **On** pour l'option **Enabled** afin d'activer l'utilisation du module pour le test de l'état de santé. Vous devez appliquer la stratégie d'intégrité à FireSIGHT Management Center si vous souhaitez que vos paramètres prennent effet.



- **Alerte critique** : Si FireSIGHT Management Center ne parvient pas à communiquer avec le cloud ou à récupérer une mise à jour dans le cloud, la classification d'état de ce module passe à *Critique*.
- **Alerte d'avertissement** : Si FireSIGHT Management Center communique avec le cloud, l'état du module passe à *Avertissement* si le Management Center ne peut pas transmettre de nouvelles données de filtrage d'URL à ses périphériques gérés.

Étape 3 : Vérifier les paramètres DNS

FireSIGHT Management Center communique avec ces serveurs lors de la recherche dans le cloud :

```
database.brightcloud.com
service.brightcloud.com
```

Une fois que vous avez vérifié que les deux serveurs sont autorisés sur le pare-feu, exécutez ces

commandes sur FireSIGHT Management Center et vérifiez si Management Center est en mesure de résoudre les noms :

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.com

admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

Étape 4 : Vérifiez la connectivité aux ports requis

Les systèmes FireSIGHT utilisent les ports 443/HTTPS et 80/HTTP pour communiquer avec le service cloud.

Une fois que vous avez confirmé que Management Center est en mesure d'effectuer une nslookup réussie, vérifiez la connectivité aux ports 80 et 443 avec telnet. La base de données URL est téléchargée avec database.brightcloud.com au port 443, tandis que les requêtes URL inconnues sont effectuées à service.brightcloud.com au port 80.

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

Ce résultat est un exemple de connexion Telnet réussie à database.brightcloud.com.

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

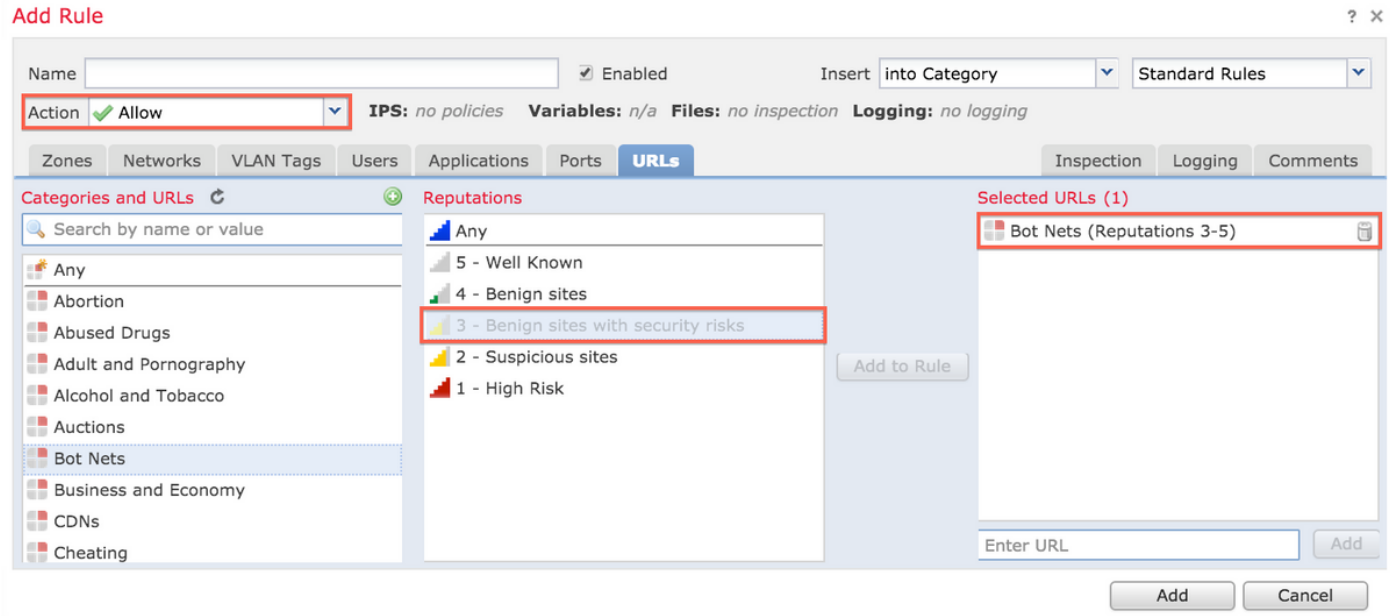
Problèmes de contrôle d'accès et de catégorisation incorrecte

Problème 1 : URL avec niveau de réputation non sélectionné autorisé/bloqué

Si vous remarquez qu'une URL est autorisée ou bloquée, mais que vous n'avez pas sélectionné le niveau de réputation de cette URL dans votre règle de contrôle d'accès, lisez cette section afin de comprendre comment fonctionne une règle de filtrage d'URL.

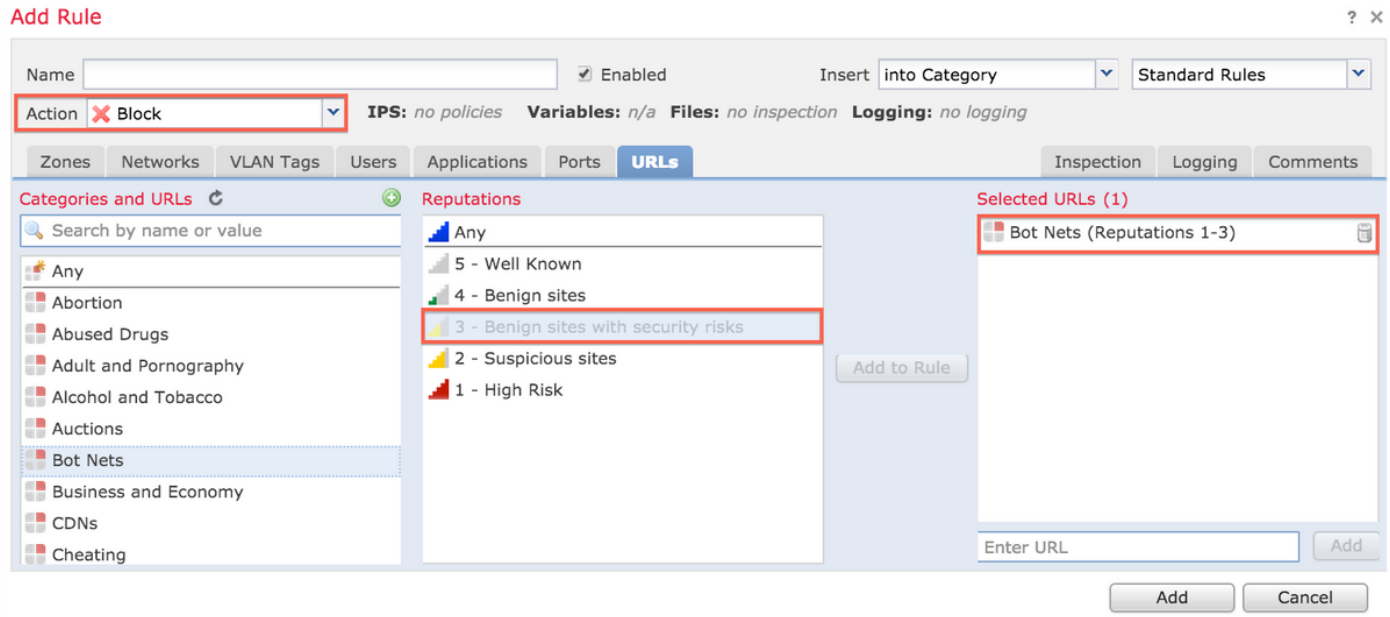
L'action de règle est Autoriser

Lorsque vous créez une règle pour **Autoriser le** trafic basé sur un niveau de réputation, la sélection d'un niveau de réputation sélectionne également tous les niveaux de réputation moins sécurisés que le niveau que vous avez initialement sélectionné. Par exemple, si vous configurez une règle pour autoriser les *sites bénignes présentant des risques de sécurité* (niveau 3), elle autorise également automatiquement les *sites bénignes* (niveau 4) et les sites *réservés* (niveau 5).



L'action de règle est Bloquer

Lorsque vous créez une règle pour **Bloquer le** trafic basé sur un niveau de réputation, la sélection d'un niveau de réputation sélectionne également tous les niveaux de réputation plus sévères que le niveau que vous avez initialement sélectionné. Par exemple, si vous configurez une règle pour bloquer les *sites dangereux* (niveau 3), elle bloque également automatiquement les *sites suspects* (niveau 2) et les sites à *haut risque* (niveau 1).



Matrice de sélection URL

Niveau de réputation sélectionné	Action de règle sélectionnée				
	Risque élevé	**Site suspect**	**Site inoffensif présentant un risque pour la sécurité**	**Site Bénigne**	**Bien Conn**
1 - Risque élevé	Bloquer, autoriser	Allow	Allow	Allow	Allow
2 - Sites suspects	Block	Bloquer, autoriser	Allow	Allow	Allow
3 - Sites inoffensifs présentant	Block	Block	Bloquer, autoriser	Allow	Allow

un risque de sécurité					
4 - Sites bénins	Block	Block	Block	Bloquer, autoriser	Allow
5 - Bien connu	Block	Block	Block	Block	Bloqu autor

Problème 2 : Le caractère générique ne fonctionne pas dans la règle de contrôle d'accès

FireSIGHT System ne prend pas en charge la spécification d'un caractère générique dans une condition d'URL. Cette condition peut ne pas être signalée sur cisco.com.

```
*cisco*.com
```

En outre, une URL incomplète peut correspondre à un autre trafic, ce qui entraîne un résultat indésirable. Lorsque vous spécifiez des URL individuelles dans des conditions d'URL, vous devez soigneusement prendre en compte tout autre trafic susceptible d'être affecté. Par exemple, considérez un scénario où vous voulez explicitement bloquer cisco.com. Cependant, la correspondance de sous-chaînes signifie que le blocage de cisco.com bloque également sanfrancisco.com, ce qui pourrait ne pas être votre intention.

Lorsque vous entrez une URL, entrez le nom de domaine et omettez les informations de sous-domaine. Par exemple, tapez cisco.com plutôt que www.cisco.com. Lorsque vous utilisez cisco.com dans une règle d'autorisation, les utilisateurs peuvent accéder à l'une des URL suivantes :

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

Problème 3 : La catégorie et la réputation des URL ne sont pas renseignées

Si une URL ne se trouve pas dans une base de données locale et que c'est la première fois que l'URL est vue dans le trafic, une catégorie ou une réputation peut ne pas être remplie. Cela signifie que la première fois qu'une URL inconnue est vue, elle ne correspond pas à la règle AC. Parfois, les recherches d'URL pour les URL fréquemment visitées peuvent ne pas être résolues lors de la première consultation d'une URL. Ce problème est résolu dans les versions 5.3.0.3, 5.3.1.2 et 5.4.0.2, 5.4.1.1.

Informations connexes

- Configuration du filtrage des URL sur un système FireSIGHT
- Support et documentation techniques - Cisco Systems