Dépannez les questions avec le Filtrage URL sur un système de FireSIGHT

Contenu

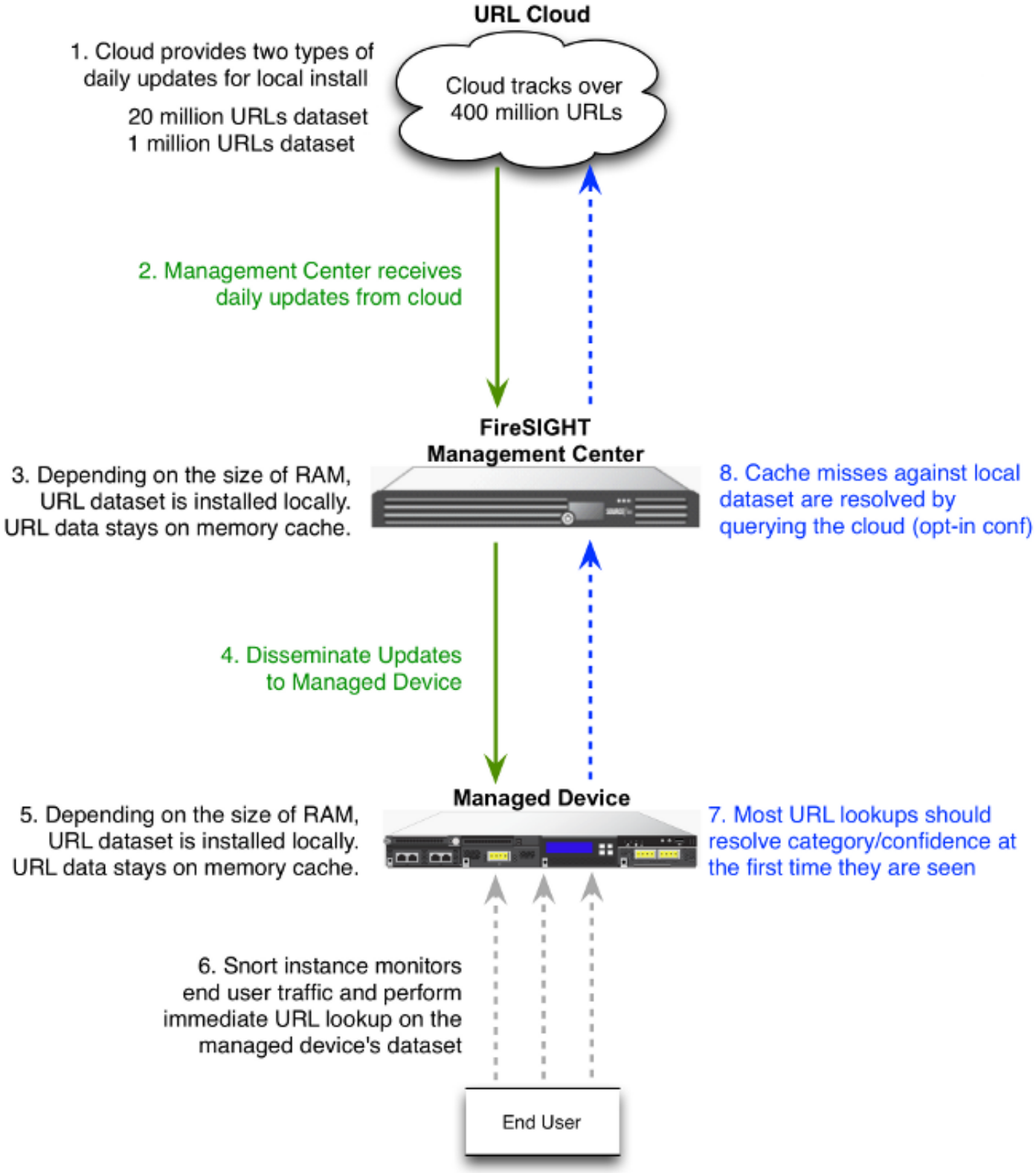
Introduction

Ce document décrit des problèmes courants avec le Filtrage URL. La caractéristique de Filtrage URL au centre de Gestion de FireSIGHT classe le trafic des hôtes surveillés et te permet par catégorie pour 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 URL, le Filtrage URL fournit un ensemble de données qui est installé sur un système de puissance de feu localement. La personne à charge sur la quantité de mémoire (RAM) disponible sur une appliance, là sont deux types d'ensembles de données :

Type d'ensemble de données	Mémoire réquise	
	Sur la version 5.3	Sur la version 5.4 ou ultérieures
20 millions d'ensemble de données URL	>2GB	>3.4 Go
1 million d'ensemble de données URL	<= 2GB	Go du <= 3.4



Problèmes de connectivité de nuage

Étape 1 : Vérifiez les permis

Le permis est-il installé ?

Vous pouvez ajouter la catégorie et les conditions basées sur réputation URL aux règles de contrôle d'accès sans Filtrage URL autorisent, toutefois vous ne pouvez pas appliquer la stratégie de contrôle d'accès jusqu'à ce que vous ajoutiez d'abord un permis de Filtrage URL au centre de

Gestion de FireSIGHT, puis l'activez sur les périphériques visés par la stratégie.

Le permis est-il expiré ?

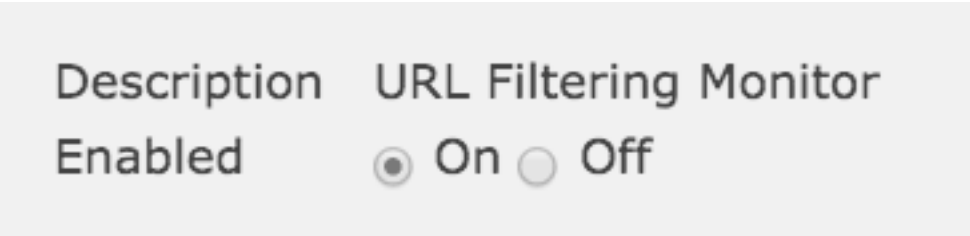
Si un permis de Filtrage URL expire, le contrôle d'accès ordonne avec la catégorie et les états basés sur réputation URL cessent de filtrer l'URLs, et le centre de Gestion de FireSIGHT ne contacte plus le service en nuage.

> **Conseil** : Lisez le Filtrage URL sur un exemple de configuration système de FireSIGHT afin d'apprendre comment activer la caractéristique de Filtrage URL sur un système de FireSIGHT et appliquer le permis de Filtrage URL sur un périphérique géré.

Étape 2 : Alertes de santés de contrôle

Les transmissions de pistes de module de moniteur de Filtrage URL entre le centre de Gestion de FireSIGHT et le Cisco opacifient, où le système obtient ses données de Filtrage URL (catégorie et réputation) pour l'URLs généralement visité. Le module de moniteur de Filtrage URL dépiste également des transmissions entre un centre de Gestion de FireSIGHT et tous les périphériques gérés où vous avez activé le Filtrage URL.

Afin d'activer le Filtrage URL surveillez le module, vont à la page de **configuration de politique de santés**, choisissent le **moniteur de Filtrage URL**. Cliquez sur **en fonction la** case d'option pour l'option **activée** afin d'activer l'utilisation du module pour le test d'état de santés. Vous devez s'appliquer la politique sanitaire au centre de Gestion de FireSIGHT si vous voulez que vos configurations les prennent effet.



- **Alerte essentielle** : Si le centre de Gestion de FireSIGHT ne communique pas avec succès avec ou ne récupère pas une mise à jour du nuage, la classification d'état pour des modifications de ce module à *essentiel*.
- **Alerte d'avertissement** : Si le centre de Gestion de FireSIGHT communique avec succès avec le nuage, les changements d'état de module à *avertir* si le centre de Gestion ne peut pas pousser de nouvelles données de Filtrage URL à ses périphériques gérés.

Étape 3 : Configurations de DN de contrôle

Un centre de Gestion de FireSIGHT communique avec ces serveurs pendant la consultation de nuage :

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

Une fois que vous vous assurez que les deux serveurs sont permis sur le Pare-feu, exécutez ces commandes au centre de Gestion de FireSIGHT et les vérifiez si le centre de Gestion peut résoudre les noms :

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

Étape 4 : Connectivité de contrôle aux ports requis

Les systèmes de FireSIGHT emploient les ports 443/HTTPS et 80/HTTP afin de communiquer avec le service en nuage.

Une fois que vous confirmez que le centre de Gestion peut exécuter un `nslookup` réussi, vérifiez la Connectivité au port 80 et au port 443 avec le `telnet`. La base de données URL est téléchargée avec `database.brightcloud.com au` port 443, alors que les requêtes inconnues URL sont faites chez `service.brightcloud.com au` port 80.

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

Cette sortie est un exemple d'une connexion réussie de `telnet à database.brightcloud.com`.

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

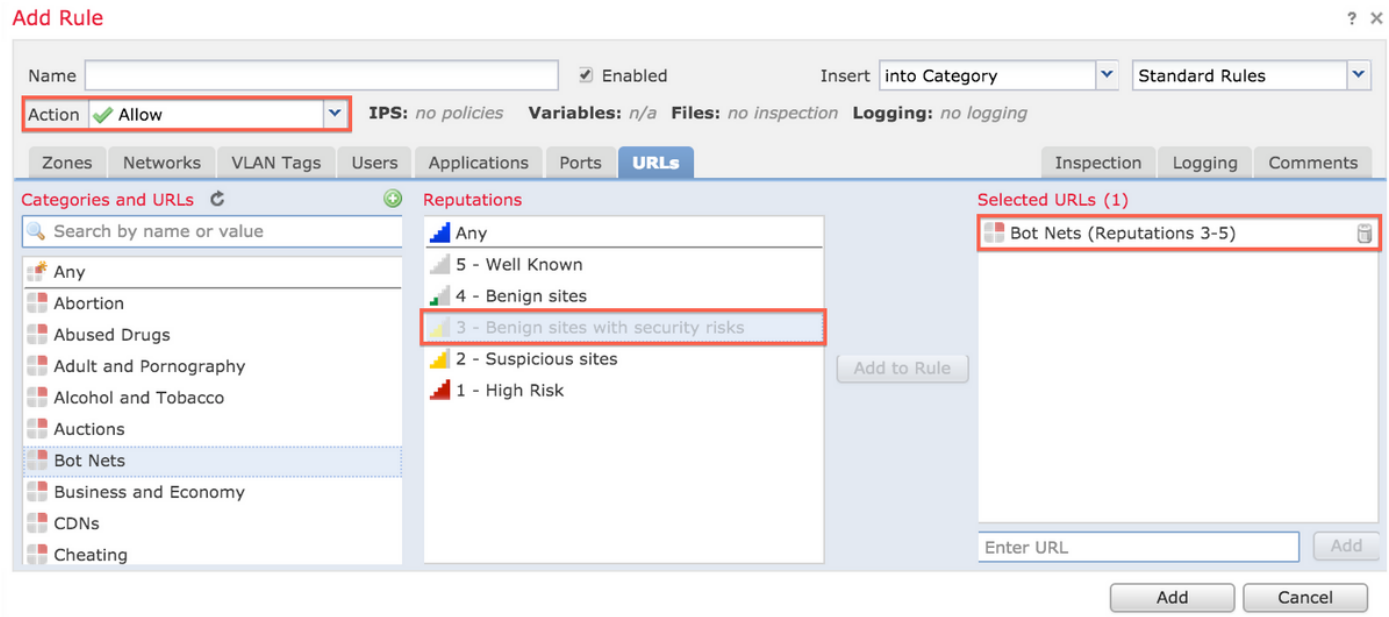
Contrôle d'accès et questions de Miscategorization

Problème 1 : L'URL avec le niveau non sélectionné de réputation est permis/bloqué

Si vous notez un URL est permis ou bloqué, mais vous n'avez pas sélectionné le niveau de réputation de cet URL dans votre règle de contrôle d'accès, lisez cette section afin de comprendre comment une règle de Filtrage URL fonctionne.

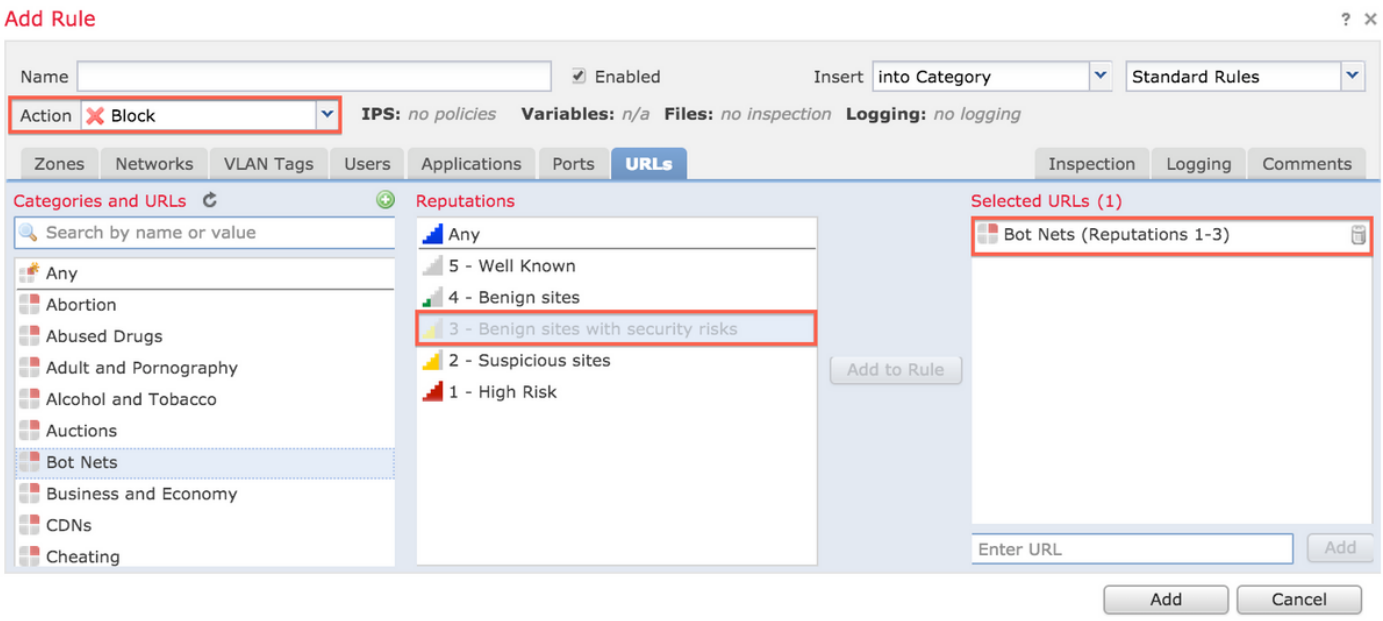
L'action de règle est laissent

Quand vous créez une règle **de permettre le** trafic basé sur un niveau de réputation, la sélection d'un niveau de réputation sélectionne également tous les niveaux de réputation moins sécurisé que le niveau que vous avez initialement sélectionné. Par exemple, si vous configurez une règle de permettre les *sites bénins avec des risques de sécurité* (niveau 3), il permet également automatiquement les *sites bénins* (niveau 4) et *réputé* (des sites de niveau 5).



L'action de règle est bloc

Quand vous créez une règle **de bloquer le** trafic basé sur un niveau de réputation, la sélection d'un niveau de réputation sélectionne également tous les niveaux de réputation plus graves que le niveau que vous avez initialement sélectionné. Par exemple, si vous configurez une règle de bloquer les *sites bénins avec des risques de sécurité* (niveau 3), il bloque également automatiquement les *sites méfiants* (niveau 2) et *risque fort* (sites de niveau 1).



Matrice de sélection URL

Niveau sélectionné de réputation	Action sélectionnée de règle				
	Risque fort	**Site méfiant**	**Site bénin avec le risque de sécurité**	**Site bénin**	**Réput**
1 - Risque fort	Le bloc, laissent	Laissez	Laissez	Laissez	Laisse
2 - Sites méfiants	Bloc	Le bloc, laissent	Laissez	Laissez	Laisse
3 - Sites bénins avec le risque de sécurité	Bloc	Bloc	Le bloc, laissent	Laissez	Laisse
4 - Sites bénins	Bloc	Bloc	Bloc	Le bloc, laissent	Laisse
5 - Réputé	Bloc	Bloc	Bloc	Bloc	Le blo laisse

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

Le système de FireSIGHT ne prend en charge pas la spécification d'un masque en état URL. Cette condition pourrait pour alerter sur `cisco.com`.

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

En outre, un URL inachevé pourrait s'assortir contre l'autre trafic qui entraîne un résultat peu désiré. Quand vous spécifiez l'URLs individuel en états URL, vous devez soigneusement considérer l'autre trafic qui pourrait être affecté. Par exemple, considérez un scénario où vous voulez bloquer explicitement `cisco.com`. Cependant, apparier de sous-chaîne signifie que cela le blocage de `cisco.com` bloque également `sanfrancisco.com`, qui ne pourrait pas être votre intention.

Quand vous écrivez un URL, écrivez le nom de domaine et omettez les informations de sous-domaine. Par exemple, type `cisco.com` plutôt que `www.cisco.com`. Quand vous utilisez `cisco.com` dans une règle d' **autoriser**, les utilisateurs pourraient parcourir à l'un de ces URLs :

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

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

Si un URL n'est pas dans une base de données locale et c'est la première fois que l'URL est vu dans le trafic, une catégorie ou une réputation ne pourrait pas être remplie. Ceci signifie que la première fois qu'un URL inconnu est vu, il n'apparie pas la règle à C.A. Parfois les consultations URL pour l'URLs généralement visité ne pourraient pas les résoudre à la première fois qu'un URL est vu. Cette question est réparée sur la version 5.3.0.3, 5.3.1.2, et 5.4.0.2, 5.4.1.1.

Informations connexes

- Configuration de Filtrage URL sur un système de FireSIGHT
- Support et documentation techniques - Cisco Systems