L'adresse IP est bloquée ou mise sur la liste noire par les renseignements de sécurité d'un système de Cisco FireSIGHT

ID de document : 117993

Mis à jour : Oct. 21, 2015

Contribué par Nazmul Rajib, ingénieur TAC Cisco.

PDF de téléchargement
Copie
Commentaires

Produits connexes

- Centre 750 de Gestion de Cisco FireSIGHT
- Centre 3500 de Gestion de Cisco FireSIGHT
- Centre 1500 de Gestion de Cisco FireSIGHT
- Centre de Gestion de Cisco FireSIGHT

Contenu

Introduction

La caractéristique de renseignements de sécurité te permet pour spécifier le trafic qui peut traverser votre réseau basé sur la source ou l'adresse IP de destination. C'est particulièrement utile si vous voulez mettre - refusez le trafic à et de - les adresses IP sur la liste noire spécifiques, avant que le trafic soit soumis à l'analyse par des règles de contrôle d'accès. Ceci documente décrit comment manipuler des scénarios quand une adresse IP est bloquée ou mise sur la liste noire par un système de Cisco FireSIGHT.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance au centre de Gestion de Cisco FireSIGHT.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Centre de Gestion de Cisco FireSIGHT
- Appliance de Cisco FirePOWER
- Cisco ASA avec le module de FirePOWER (SFR)
- Version de logiciel 5.2 ou plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Différence entre le flux d'intelligence et la liste d'intelligence

Il y a deux manières d'utiliser la caractéristique de renseignements de sécurité dans un système de FireSIGHT :

Flux de renseignements de sécurité

Un flux de renseignements de sécurité est une collection dynamique d'adresses IP que le centre de la défense télécharge d'un serveur de HTTP ou HTTPS. Pour vous aider à établir des listes noires, Cisco fournit le *flux de renseignements de sécurité*, qui représente des adresses IP déterminées par l'équipe de recherche de vulnérabilité (VRT) pour avoir une réputation pauvre.

Liste de renseignements de sécurité

Une liste de renseignements de sécurité, contrastée avec un flux, est une liste d'adresses IP statique simple que vous téléchargez manuellement au centre de Gestion de FireSIGHT.

L'adresse IP légitime est bloquée ou mise sur la liste noire

Vérifiez si une adresse IP est dans le flux de renseignements de sécurité

Si une adresse IP est bloquée par la liste noire de flux de renseignements de sécurité, vous pouvez suivre les étapes ci-dessous pour vérifier ceci :

Étape 1 : Accédez au CLI de l'appliance de FirePOWER ou du module de service.

Étape 2 : Exécutez la commande suivante. Remplacez le `<IP_Address>` par l'adresse IP que vous voulez rechercher :

```
admin@Firepower:~$ grep <IP_Address> /var/sf/iprep_download/*.blf
```

Par exemple, si vous voulez rechercher l'adresse IP 198.51.100.1, exécutez la commande suivante :

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

Si cette commande renvoie n'importe quelle correspondance pour l'adresse IP que vous avez fournie, elle indique que l'adresse IP est présente sur la liste noire de flux de renseignements de sécurité.

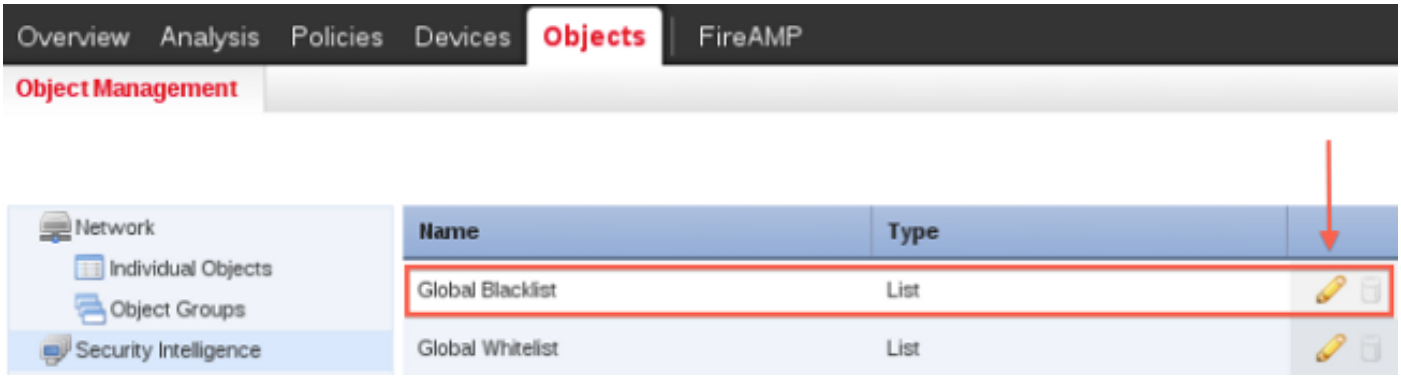
Vérifiez la liste noire

Pour trouver une liste des adresses IP qui pourraient être mises sur la liste noire, suivez les étapes ci-dessous :

Étape 1 : Access à l'interface web du centre de Gestion de FireSIGHT.

Étape 2 : Naviguez vers les **objets > la Gestion > les renseignements de sécurité d'objet**.

Étape 3 : Cliquez sur en fonction l'icône de *crayon* pour ouvrir ou éditer la **liste noire globale**. Une fenêtre d'afficher avec une liste d'adresses IP apparaît.



Travail avec une adresse IP bloquée ou mise sur la liste noire

Si une adresse IP particulière est bloquée ou mise sur la liste noire par le flux de renseignements de sécurité, vous pouvez considérer des options suivantes l'unes des de le permettre.

Option 1 : Renseignements de sécurité Whitelists

Vous pouvez whitelist une adresse IP qui est mise sur la liste noire par des renseignements de sécurité. Un whitelist ignore sa liste noire. Le système de FireSIGHT évalue le trafic avec une source ou une adresse IP whitelisted de destination utilisant des règles de contrôle d'accès, même si une adresse IP est également mise sur la liste noire. Par conséquent, vous pouvez utiliser un whitelist quand une liste noire est encore utile, mais êtes trop large dans la portée et inexactement les blocs trafiquent que vous voulez examiner.

Par exemple, si un flux honorable bloque incorrectement votre accès à une ressource essentielle mais est globalement utile à votre organisation, vous pouvez whitelist les adresses IP incorrectement classifiées seulement, plutôt qu'enlevant le flux de totalité de la liste noire.

> **Attention** : Après que vous apportiez n'importe quelle modification dans une stratégie de contrôle d'accès, vous devez réappliquer la stratégie aux périphériques gérés.

Option 2 : Imposez le filtre de renseignements de sécurité par zone de Sécurité

Pour la finesse accrue, vous pouvez imposer le filtrage de renseignements de sécurité basé en fonction si la source ou l'adresse IP de destination dans une connexion réside dans une zone de Sécurité particulière.

Pour étendre l'exemple de whitelist ci-dessus, vous pourriez whitelist les adresses IP incorrectement classifiées, mais d'autre part limiter l'objet de whitelist utilisant une zone de Sécurité utilisée par ceux dans votre organisation qui doit accéder à ces adresses IP. Que la manière, seulement ceux avec un besoin d'affaires peut accéder aux adresses IP whitelisted. En tant qu'autre exemple, vous pourriez vouloir employer un tiers flux de Spam pour mettre le trafic sur la liste noire sur une zone de degré de sécurité de serveur de mail.

Option 3 : Surveillez, plutôt que la liste noire

Si vous n'êtes pas sûr si vous voulez mettre une adresse IP particulière ou un ensemble sur la liste noire d'adresses, vous pouvez utiliser une configuration « réservée au moniteur », qui permet au système pour passer la connexion assortie aux règles de contrôle d'accès, mais vous connectez également la correspondance à la liste noire. Notez que vous ne pouvez pas placer la liste noire globale à réservé au moniteur

Considérez un scénario où vous voulez examiner un tiers flux avant que vous implémentiez le blocage utilisant ce flux. Quand vous placez le flux à réservé au moniteur, le système permet les connexions qui auraient été bloquées pour être encore analysées par le système, mais se connecte également un enregistrement de chacune de ces connexions pour votre évaluation.

Étapes pour configurer les renseignements de sécurité avec la configuration « réservée au moniteur » :

1. Sur l'onglet de **renseignements de sécurité** dans une stratégie de contrôle d'accès, cliquez sur l'icône se connectante. La boîte de dialogue d'options de liste noire apparaît.
2. Sélectionnez la case de **connexions de log** pour se connecter des événements de début-de-connexion quand le trafic remplit des conditions de renseignements de sécurité.
3. Spécifiez où envoyer des événements de connexion.
4. Cliquez sur OK pour placer vos options se connectantes. L'onglet de renseignements de sécurité apparaît de nouveau.
5. Cliquez sur **Save**. Vous devez appliquer la stratégie de contrôle d'accès pour que vos modifications les prennent effet.

Option 4 : Centre d'assistance technique Cisco de contact

Vous pouvez toujours entrer en contact avec le centre d'assistance technique Cisco, si :

- Vous avez des questions avec les options ci-dessus 1, 2 ou 3.
- Vous voulez davantage de recherche et d'analyse sur une adresse IP qui est mise sur la liste noire par des renseignements de sécurité.
- Vous voulez une explication pourquoi l'adresse IP est mise sur la liste noire par des renseignements de sécurité.

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Oct. 21, 2015
ID de document : 117993