L'adresse IP est bloquée ou mise en liste noire par Security Intelligence d'un système Cisco FireSIGHT

Contenu

Introduction

La fonction Security Intelligence vous permet de spécifier le trafic qui peut traverser votre réseau en fonction de l'adresse IP source ou de destination. Ceci est particulièrement utile si vous voulez mettre en liste noire - refuser le trafic à destination et en provenance - des adresses IP spécifiques, avant que le trafic ne soit soumis à une analyse par les règles de contrôle d'accès. Ce document décrit comment gérer des scénarios lorsqu'une adresse IP est bloquée ou mise sur liste noire par un système Cisco FireSIGHT.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître Cisco FireSIGHT Management Center.

Components Used

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

- Cisco FireSIGHT Management Center
- Appareil Cisco Firepower

- Cisco ASA avec module Firepower (SFR)
- Version de logiciel 5.0 ou ultérieure

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. If your network is live, make sure that you understand the potential impact of any command.

Différence entre le flux Intelligence et la liste Intelligence

Il existe deux façons d'utiliser la fonction Security Intelligence dans un système FireSIGHT :

Flux Security Intelligence

Un flux Security Intelligence est un ensemble dynamique d'adresses IP que le Centre de défense télécharge à partir d'un serveur HTTP ou HTTPS. Pour vous aider à créer des listes noires, Cisco fournit le *flux Security Intelligence*, qui représente les adresses IP jugées médiocres par l'équipe de recherche sur les vulnérabilités (VRT).

Liste Security Intelligence

Une liste Security Intelligence, par opposition à un flux, est une simple liste statique d'adresses IP que vous téléchargez manuellement vers FireSIGHT Management Center.

L'adresse IP autorisée est bloquée ou mise en liste noire

Vérifier si une adresse IP figure dans le flux Security Intelligence

Si une adresse IP est bloquée par la liste noire Security Intelligence Feed, vous pouvez suivre les étapes ci-dessous pour vérifier ceci :

Étape 1 : Accédez à l'interface de ligne de commande du périphérique Firepower ou du module de service.

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

```
admin@Firepower:~$ grep
```

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 une correspondance pour l'adresse IP que vous avez fournie, elle

indique que l'adresse IP figure sur la liste noire Security Intelligence Feed.

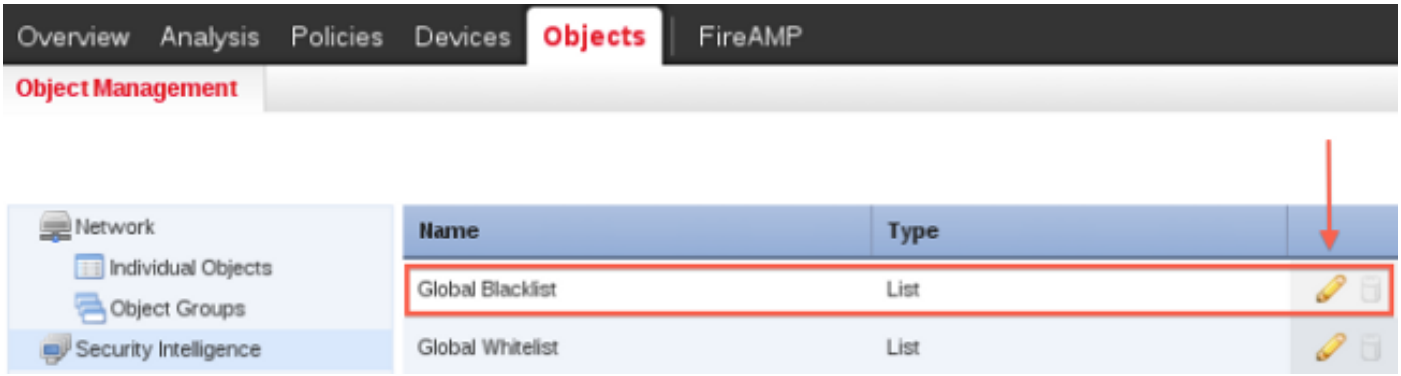
Vérifier la liste noire

Pour trouver une liste des adresses IP qui peuvent être mises en liste noire, procédez comme suit :

Étape 1 : Accès à l'interface Web de FireSIGHT Management Center.

Étape 2 : Accédez à **Objets > Gestion des objets > Intelligence de sécurité**.

Étape 3 : Cliquez sur l'icône *au crayon* pour ouvrir ou modifier la **liste de blocage globale**. Une fenêtre contextuelle contenant une liste d'adresses IP s'affiche.



Utilisation d'une adresse IP bloquée ou mise en liste noire

Si une adresse IP particulière est bloquée ou mise sur liste noire par Security Intelligence Feed, vous pouvez envisager l'une des options suivantes pour l'autoriser.

Option 1 : Listes blanches de Security Intelligence

Vous pouvez blanchir une adresse IP qui est mise sur liste noire par Security Intelligence. Une liste blanche remplace sa liste noire. Le système FireSIGHT évalue le trafic avec une adresse IP source ou de destination liste blanche à l'aide de règles de contrôle d'accès, même si une adresse IP est également mise sur liste noire. Par conséquent, vous pouvez utiliser une liste blanche lorsqu'une liste noire est toujours utile, mais a une portée trop large et bloque incorrectement le trafic que vous voulez inspecter.

Par exemple, si un flux fiable bloque indûment votre accès à une ressource vitale mais est globalement utile à votre organisation, vous pouvez uniquement blanchir les adresses IP incorrectement classées, plutôt que de supprimer le flux entier de la liste noire.

> **Attention** : Une fois que vous avez modifié une stratégie de contrôle d'accès, vous devez réappliquer la stratégie aux périphériques gérés.

Option 2 : Appliquer le filtre Security Intelligence par zone de sécurité

Pour obtenir une granularité supplémentaire, vous pouvez appliquer le filtrage Security Intelligence en fonction du fait que l'adresse IP source ou de destination d'une connexion réside

dans une zone de sécurité particulière.

Pour étendre l'exemple de liste blanche ci-dessus, vous pouvez répertorier les adresses IP incorrectement classées, puis restreindre l'objet de liste blanche à l'aide d'une zone de sécurité utilisée par les personnes de votre organisation qui doivent accéder à ces adresses IP. De cette manière, seules les personnes ayant des besoins professionnels peuvent accéder aux adresses IP de liste blanche. Autre exemple, vous pouvez utiliser un flux de spam tiers pour mettre le trafic sur une liste noire dans une zone de sécurité du serveur de messagerie.

Option 3 : Surveiller plutôt que de bloquer la liste

Si vous ne savez pas si vous voulez mettre en liste noire une adresse IP ou un ensemble d'adresses particulier, vous pouvez utiliser un paramètre de ” de surveillance uniquement “, qui permet au système de transmettre la connexion correspondante aux règles de contrôle d'accès, mais enregistre également la correspondance dans la liste noire. Notez que vous ne pouvez pas définir la liste noire globale sur surveillance uniquement

Considérez un scénario dans lequel vous voulez tester un flux tiers avant d'implémenter le blocage à l'aide de ce flux. Lorsque vous configurez le flux en mode surveillance seule, le système autorise les connexions qui auraient été bloquées à être analysées plus avant par le système, mais enregistre également un enregistrement de chacune de ces connexions pour votre évaluation.

Étapes de configuration de Security Intelligence avec le paramètre de surveillance uniquement :

1. Dans l'onglet **Security Intelligence** d'une stratégie de contrôle d'accès, cliquez sur l'icône de journalisation. La boîte de dialogue Options de liste noire s'affiche.
2. Activez la case à cocher **Connexions du journal** pour consigner les événements de début de connexion lorsque le trafic satisfait aux conditions de Security Intelligence.
3. Spécifiez où envoyer les événements de connexion.
4. Cliquez sur **OK** pour définir vos options de journalisation. L'onglet Security Intelligence s'affiche à nouveau.
5. Click **Save**. Vous devez appliquer la stratégie de contrôle d'accès pour que vos modifications prennent effet.

Option 4 : Contactez le centre d'assistance technique Cisco

Vous pouvez toujours contacter le centre d'assistance technique de Cisco si :

- Vous avez des questions sur les options 1, 2 ou 3 ci-dessus.
- Vous souhaitez approfondir les recherches et les analyses sur une adresse IP mise sur liste noire par Security Intelligence.
- Vous voulez savoir pourquoi l'adresse IP est mise sur liste noire par Security Intelligence.