Configurer la fonction Ignorer la liste du collecteur de flux

Table des matières

Introduction

Ce document décrit comment configurer votre collecteur de flux SNA pour rejeter le flux net entrant d'un exportateur particulier en utilisant Ignorer la liste.

Informations générales

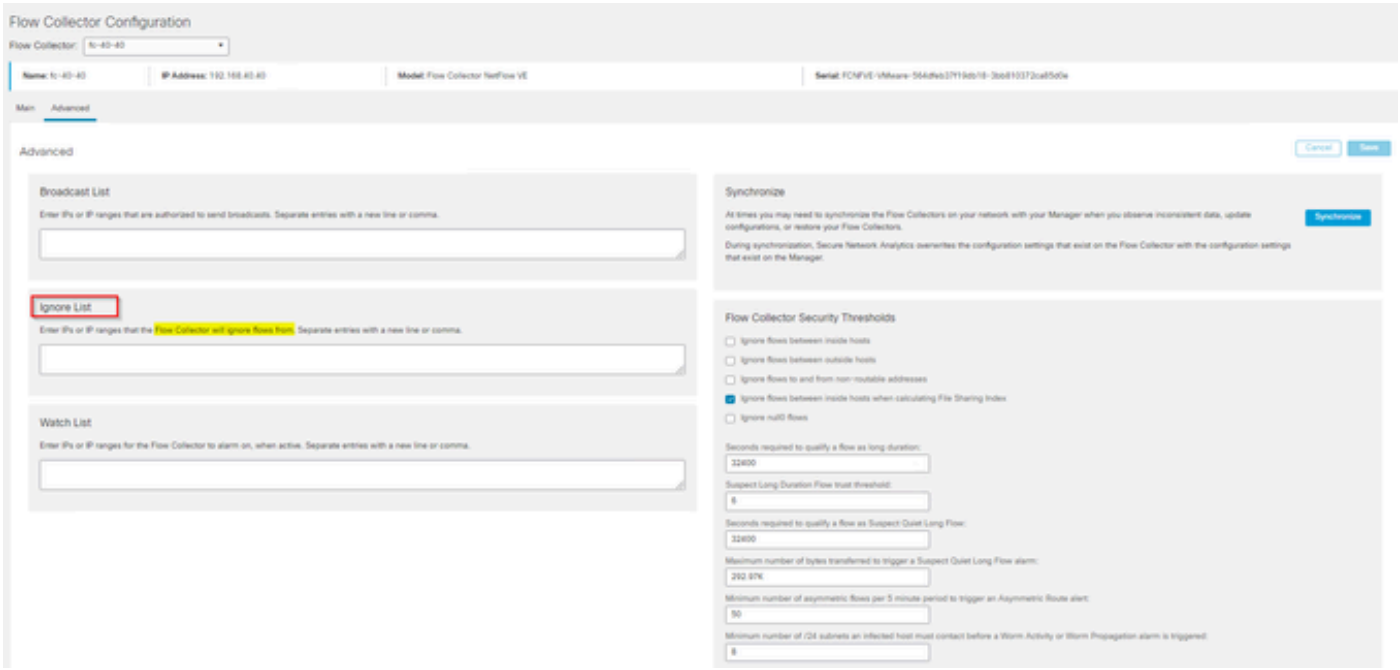
Souvent, la question est posée : « Existe-t-il un moyen de demander à mon collecteur de flux SNA de rejeter le flux net entrant d'un exportateur particulier ? »

La réponse est oui, cela se fait par l'utilisation de la fonction "Ignorer la liste" des collecteurs de flux.

Configurer

La fonctionnalité de liste d'exclusion est spécifique au collecteur de flux. Dans la version ultérieure de SNA 7.x, cette fonctionnalité est disponible dans la page de configuration du collecteur de flux de l'interface utilisateur Web de SNA Manager.

Utilisez cette page pour spécifier un nombre illimité d'hôtes ou de sous-réseaux pour lesquels le collecteur de flux ignore complètement le trafic. Si le collecteur de flux détecte un trafic attribuable à ces adresses IP, il exclut ce trafic de tout graphique ou table. Assurez-vous que vous pouvez faire confiance à tout le trafic en provenance ou à destination des hôtes pour qu'il soit ignoré.Secure Network Analytics n'analyse pas ce trafic ni tout trafic qui est usurpé pour inclure l'un de ces hôtes. Si une attaque est lancée sur votre réseau impliquant l'un de ces hôtes/sous-réseaux, le collecteur de flux ne peut pas le signaler.



FAQ

Quel est l'effet de l'option Ignorer la liste sur les calculs de flux par seconde (FPS) pour les licences Smart ?

Réponse : L'ajout d'adresses IP ou de plages d'hôtes à la liste d'exclusion empêche efficacement ces flux de compter par rapport au taux FPS calculé envoyé au SMC et utilisé pour les rapports de licence Smart. Les flux ne sont plus affichés/comptés dans le graphique de tendance de flux affiché sur le tableau de bord SMC.

Comment la fonction de liste d'exclusion est-elle utilisée lors du traitement du flux NVM lorsque le client est en mode de tunnel partagé ?

Un client peut configurer AnyConnect pour qu'il nous envoie du trafic sur le réseau et hors réseau (ou tunnel partagé). Le trafic hors réseau utilise l'adresse IP locale du point d'extrémité qui contient très probablement des adresses IP qui se chevauchent. SNA ne prend pas en charge les adresses IP qui se chevauchent, il a donc été suggéré d'utiliser la fonction de liste Ignorer pour contourner le problème du split tunnel, préservant ainsi l'avantage des flux basés sur NVM pour les détections.

Dans ce cas d'utilisation, nous configurons la « liste d'exclusion » pour empêcher les flux NVM hors réseau de sortir du cache de flux → flow_stats, Flow Search, Custom Security Events

1. Ajoutez l'adresse IP et le masque de réseau (par exemple, ajoutez 192.168.1.0/24, 127.0.0.1/24) dans la liste Ignorer
2. Vérifiez que les flux nvm_flows contiennent toujours les flux NVM
3. Vérifiez que flow_stats n'a pas les flux NVM si l'adresse IP src ou dst figure dans la liste Ignorer

Puis-je utiliser une liste d'exclusion pour ignorer les flux provenant d'un exportateur entier ? Non,

parce que la liste d'exclusion est basée sur des données de flux et non sur des données d'exportateur, ajouter une adresse IP d'exportateur à la liste d'exclusion ignorerait effectivement les données de flux lorsque l'adresse IP de l'exportateur était répertoriée comme source ou destination du flux, au lieu d'ignorer tous les enregistrements de flux provenant de cet exportateur particulier

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.