

Configuration des événements de sécurité SLF et SQLF dans Secure Analytics

Table des matières

[Introduction](#)

[Informations générales](#)

[Réglage/configuration](#)

[Solution](#)

Introduction

Ce document décrit deux paramètres qui peuvent être utilisés pour régler les événements de sécurité SLF (suspect long flow) et SQLF (suspect quiet long flow).

Informations générales

Un événement Suspect Long Flow est un type spécifique d'événement de sécurité généré par Secure Analytics et conçu pour détecter des conversations plus longues que la normale entre les hôtes. Il existe deux types différents d'événement de flux long suspect ; Flux long suspect et Flux long silencieux suspect.

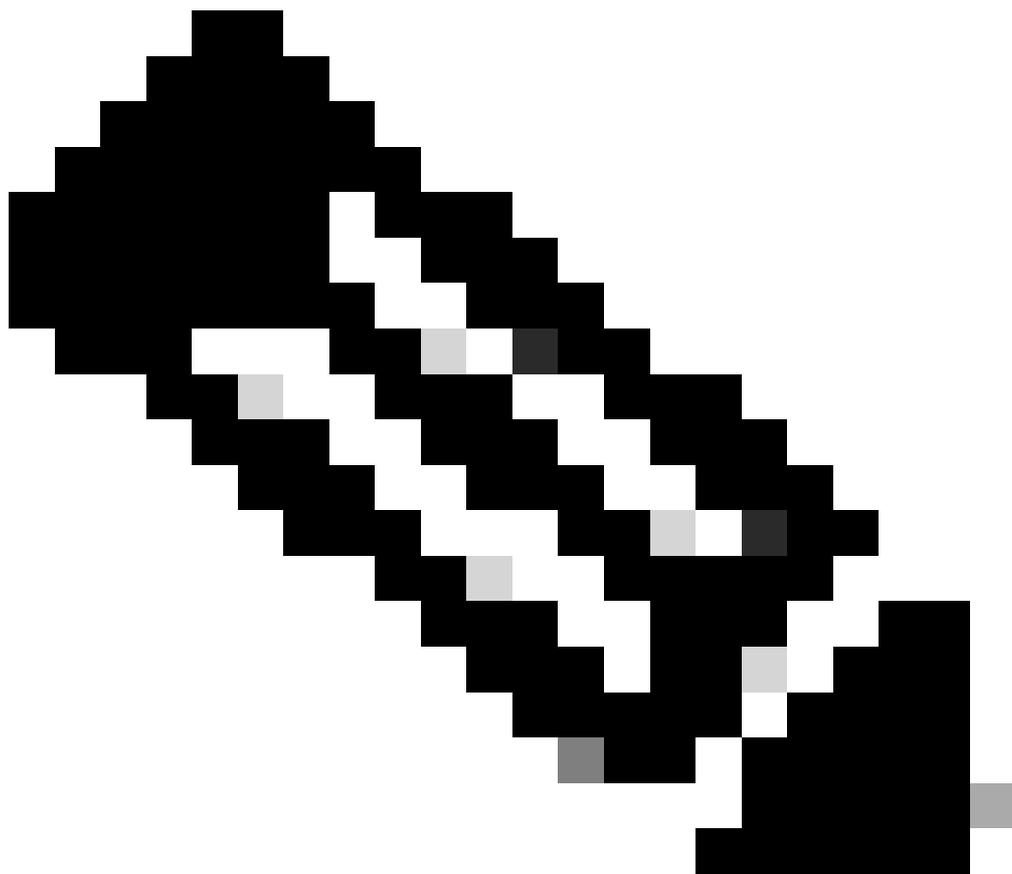
Considérez que vous connectez votre ordinateur portable à votre ordinateur personnel via un VPN caché pendant 3 jours, mais ni l'ordinateur personnel ni l'ordinateur portable n'ont normalement de connexions à flux long. Le collecteur de flux détecte cette anomalie et déclenche un événement de sécurité en fonction de la quantité de trafic transmise et de la durée du flux. Ces événements sont destinés à identifier les flux longs et les flux longs qui transitent un trafic minimal.

Réglage/configuration

Il existe principalement deux paramètres de configuration du collecteur de flux qui sont chargés de contrôler le comportement de ces deux événements.

Ces paramètres peuvent être réglés en accédant à la page Configure > Flow Collectors > Advanced dans l'interface Web de l'appliance de gestion.

- Les secondes nécessaires pour qualifier un flux en tant que paramètre de longue durée contrôlent le comportement de l'événement de long flux suspect.



Remarque : Cette option de configuration de webUI définit le paramètre `long_flow_duration` dans le fichier de configuration `lc_threshold.txt` des collecteurs de flux.

-
- Les secondes nécessaires pour qualifier un flux comme paramètre de flux long silencieux suspect contrôlent le comportement de l'événement de flux long silencieux suspect.



Remarque : Cette option de configuration de webUI définit le paramètre `quiet_long_flow_duration` dans le fichier de configuration `lc_threshold.txt` des collecteurs de flux.

La valeur par défaut pour les deux compteurs est 32400 secondes (9 heures).



Remarque : En ce qui concerne le changement de ces compteurs, CDET connexe :

ID de bogue Cisco [CSCwm05128](#)



Avertissement : Cela concerne uniquement la version 7.5.1 ou les versions précédentes.

Ce défaut impose qu'un débit long silencieux suspect soit d'abord également un débit long suspect. Cela signifie que si vous remplacez les secondes requises pour qualifier un flux comme flux long silencieux suspect par une durée plus courte que les secondes requises pour qualifier un flux comme paramètre de longue durée, des résultats inattendus sont probables.

Si vous modifiez l'un de ces paramètres avancés ou les deux, la détection des flux longs peut échouer.

Étant donné qu'un écoulement long silencieux doit par définition être également un écoulement long, la logique dans la gestion appropriée de ces deux paramètres est d'abord que l'écoulement dépasse les exigences d'écoulement long avant de tester pour qu'il soit un écoulement long silencieux.

Par exemple, si la valeur par défaut de `long_flow_duration` est conservée à 9 heures et que la valeur de `quiet_long_flow_duration` est définie sur une valeur inférieure, par exemple 8 heures, le

moteur ne déclenche pas d'événement de flux de longue durée tant que le flux n'est pas d'une durée d'au moins 9 heures.

Si la valeur par défaut de `long_flow_duration` est de 9 heures et que la valeur de `quiet_long_flow_duration` est de 10 heures, cette configuration désactive l'événement de flux de longue durée silencieux (à moins qu'il ne s'agisse d'une exportation unique ayant une durée $>$ `quiet_long_flow_duration` de 10 heures).

Solution

Ces deux paramètres avancés doivent être définis sur la même valeur souhaitée ou la valeur `quiet_long_flow_duration` doit toujours être \geq `long_flow_duration`.

The screenshot shows the 'Secure Network Analytics' interface for configuring a 'Flow Collector'. The 'Advanced' tab is active, showing several configuration sections:

- Broadcast List:** A text input field for entering authorized IP ranges.
- Ignore List:** A text input field for entering IP ranges to ignore.
- Watch List:** A text input field for entering IP ranges to monitor.
- Synchronize:** A section with a 'Synchronize' button and explanatory text.
- Flow Collector Security Thresholds:** A section with several checkboxes and input fields:
 - Ignore flows between inside hosts
 - Ignore flows between outside hosts
 - Ignore flows to and from non-routable addresses
 - Ignore flows between inside hosts when calculating File Sharing Index
 - Ignore null0 flows
 - Seconds required to qualify a flow as long duration:** 32400
 - Suspect Long Duration Flow trust threshold: 6
 - Seconds required to qualify a flow as Suspect Quiet Long Flow:** 32400
 - Maximum number of bytes transferred to trigger a Suspect Quiet Long Flow alarm: 292.97K
 - Minimum number of asymmetric flows per 5 minute period to trigger an Asymmetric Route alert: 50
 - Minimum number of /24 subnets an infected host must contact before a Worm Activity or Worm Propagation alarm is triggered: 8

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.