# Exemples de configuration de récapitulation IPS

## Contenu



## Introduction

Ce document fournit des explications, des avantages, et des exemples pour la configuration de la récapitulation sur le Système de protection contre les intrusions Cisco (IPS).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité adaptable Cisco (ASA) 5500 ou modules du Système de protection contre les intrusions Cisco 5500x (IPS)
- IPS 4200, 4300, ou appliances IPS de gamme 4500
- Module NME-IPS
- Alertes de signature IPS

### Composants utilisés

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

- Modules ASA 5500 ou 5500x IPS
- IPS 4200, appliances IPS de gamme 4300 ou 4500
- Module NME-IPS

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.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

## Informations générales

La récapitulation IPS fournit des modes pour agréger des événements dans une alerte simple, de sorte que le volume d'alertes envoyées par le capteur puisse être diminué. Chaque signature est créée avec les par défaut qui reflètent un comportement préféré et normal. Cependant, chaque signature a les paramètres spéciaux qui influencent comment des alertes sont manipulées, ainsi le comportement par défaut des signatures peut être accordé dans les contraintes pour chaque type de moteur.

Des actions de récapitulation et d'événement sont traitées après que l'engine de méta ait traité les événements composants. Ceci permet le capteur d'observer pour l'activité suspecte au-dessus d'une gamme d'événements.

L'agrégation de base fournit deux modes :

- **Mode simple** - configure un nombre de hits de seuil pour une signature qui doit être rencontrée avant que l'alerte soit envoyée.
- **Mode avancé** - configure un nombre de hits de seuil par seconde (compte de synchronisé-intervalle) pour une signature qui doit être rencontrée avant que l'alerte soit envoyée.

### Options de récapitulation

- **feu-tout** - Se déclenche une alerte chaque fois que la signature est déclenchée. Si le seuil est placé pour la récapitulation, des alertes sont déclenchées pour chaque exécution jusqu'à ce que la récapitulation se produise. Après que les débuts de récapitulation, seulement une alerte pour chaque intervalle récapitulatif se déclenche pour chaque positionnement d'adresse. Des alertes pour d'autres positionnements d'adresse sont tout vues ou séparément récapitulées. La signature retourne à feu-**tout** mode après une période sans alertes pour cette signature.
- **résumé** - Se déclenche une alerte la première fois qu'une signature est déclenchée. Des alertes supplémentaires pour cette signature sont récapitulées pour la durée de l'intervalle

récapitulatif. Seulement une alerte que chaque intervalle récapitulatif devrait se déclencher pour chaque positionnement d'adresse. Si le seuil récapitulatif global est atteint, la signature entre dans le mode de global-**récapitulation**.
- **global-récapitulation** - Se déclenche une alerte pour chaque intervalle récapitulatif. Des signatures peuvent être préconfigurées pour la global-**récapitulation**.
- **feu-une fois** - Se déclenche une alerte pour chaque positionnement d'adresse. Ce mode peut être mis à jour au mode de global-**récapitulation**.

### Récapitulation d'événement

Un scénario commun est de subir une période de spécification de base accordant afin d'identifier les signatures de alerte hyper. Il y a souvent un certain nombre de bas niveau et de signatures niveau informationnel qui ont besoin de récapitulation basée sur le mélange du trafic. Passez en revue ces signatures afin de déterminer les seuils appropriés.

> **Note**: Faites attention toutes les fois que vous réduisez la quantité d'alertes, particulièrement des alertes des signatures de à sévérité élevée. Assurez-vous que la Sécurité n'est pas compromise et que les actions appropriées sont en place pour n'importe quelle signature qui est récapitulée.

## Configuration

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

### Attaque de force brutale de SSH - Signature 3653

Les sessions rapides de Protocole Secure Shell (SSH), en alertant activement, peuvent rapidement remplir mémoire d'événement. Actuellement, des tentatives de force brutale de SSH sont refusées.

Si vous avez besoin seulement d'alertes toutes les cinq minutes, utilisez l'option **récapitulative** pour la vigilant-fréquence avec un résumé-intervalle de 300 secondes :

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 3653 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode summarize
sensor(config-sig-sig-ale-sum)# summary-interval 300
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-sum)# show settings
alert-frequency
-----------------------------------------------
summary-mode
-----------------------------------------------
summarize
-----------------------------------------------
```

```
summary-interval: 300 default: 15
summary-key: Axxx <defaulted>
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 240 <defaulted>
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

## Requête SQL excessive dans des demandes de HTTP - Signature 5474

Choisi-de la requête SQL incluse dans une demande de HTTP est une des signatures de alerte hyper les plus communes dans un déploiement de périphérie.

Afin de visualiser la signature 5474 d'heure en heure pour une paire d'attaquant/victime, utilisez feu-**une fois** option pour la vigilant-fréquence avec un résumé-intervalle de 3600 secondes :

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 5474 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 3600
sensor(config-sig-sig-ale-fir-yes)# summary-interval 3600
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir)# show settings
fire-once
-----------------------------------------------
summary-key: Axxx default: Axxx
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 3600 default: 240
summary-interval: 3600 default: 15
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

## Scanner interne ou externe d'AD TCP/UDP - Signatures 13000 13008

Dans cet exemple, la signature se déclenche quand elle détecte un scanner de Control Protocol (TCP)/Protocole UDP (User Datagram Protocol) de transport qui balaye l'ensemble d'adresses IP de destination configurées comme zone interne ou externe. Si le Manager Express IPS (IME) envoie le par défaut, les événements de à sévérité élevée comme notifications électroniques, là

pourraient être des milliers d'emails.

> **Note**: Assurez-vous que les feux ne sont pas une attaque de faux positif. Changez la configuration pour que la détection d'anomalie « apprennent le mode » pendant 48 heures, puis le déplacent de nouveau à « détectent le mode » afin de résoudre le problème.

Afin de réduire le nombre d'emails, utilisez feu-**une fois** option pour la vigilant-fréquence, avec un résumé-intervalle de 720 secondes ou une fois de toutes les 12 minutes.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 13000 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 720
sensor(config-sig-sig-ale-fir-yes)# summary-interval 720
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir-yes)# show settings
  fire-once
  -----------------------------------------------
     summary-key: Axxx <defaulted>
     specify-global-summary-threshold
     -----------------------------------------------
        yes
        -----------------------------------------------
           global-summary-threshold: 720 default: 240
           summary-interval: 720 default: 15
        -----------------------------------------------
     -----------------------------------------------
  -----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

## Informations connexes

- Configurer la fréquence vigilante
- Guides de configuration IPS
- Support et documentation techniques - Cisco Systems