Instructions de profilage des règles sur FireSIGHT System

Contenu

Introduction

Si un appareil FirePOWER ou un appareil virtuel NGIPS est sursouscrit, vous devez collecter des données supplémentaires pour déterminer quel composant du périphérique ralentit le système. Le profilage de règles permet à un système FireSIGHT de générer des données supplémentaires sur lesquelles les règles et les sous-systèmes du moteur de détection utilisent le plus de cycles de CPU. Cet article explique comment exécuter le profilage des règles sur l'appliance FireSIGHT et l'appliance virtuelle NGIPS.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez des connaissances sur les appliances FirePOWER et les modèles d'appliances virtuelles.

Components Used

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

- Appliances FirePOWER 7000, appliances 8000 et appliances virtuels NGIPS
- 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.

Avertissement : L'exécution de la commande de profilage des règles peut affecter les

performances du réseau. Par conséquent, vous ne devez exécuter cette commande que si l'assistance technique Cisco demande des données de profilage de règles.

Étapes d'exécution du profilage de règle

Étape 1 : Accédez à l'interface de ligne de commande du périphérique géré.

Étape 2 : Exécutez la commande de profilage de règle suivante pendant une période donnée. Le temps doit être compris entre 15 et 120 minutes. Dans l'exemple suivant, le script est exécuté pendant 15 minutes.

```
> system support run-rule-profiling 15
```

Étape 3 : Confirmez l'exécution de la commande. Tapez **y** et appuyez sur **Entrée**.

> **Avertissement** : la commande de profilage des règles redémarre le moteur de détection, ce qui peut affecter la fonctionnalité de détection et augmenter l'utilisation du processeur.

```
> system support run-rule-profiling 15

You are about to profile
 DE    Primary Detection Engine (94854a60-cb17-11e3-a2f5-8de07680f9f3)
 Time  15 minutes

WARNING!!  Detection Engine will be restarted.
Intrusion Detection / Prevention will be affected

Please confirm by entering 'y': y
```

Une fois l'exécution confirmée, le profilage des règles commence. Le temps nécessaire pour terminer le profilage compte jusqu'à zéro minute.

```
Restarting DE for profiling...done
Profiling for 15 more minutes...
```

Une fois terminé, l'invite du shell revient.

```
Restarting DE for profiling...done
Profiling...done
Restarting DE with original configuration...in progress
>
```

Étape 4 : La commande de profilage de règle génère un fichier .tgz. vous pouvez trouver le fichier en exécutant la commande suivante dans le shell.

```
> system file list
May 12 15:53 99364308 profiling.94854a60-cb17-11e3-a2f5-8de07680f9f3.1399909945.tgz
```

Étape 5 : Fournir le fichier au support technique Cisco pour une analyse plus approfondie.