

Collecte de statistiques de représentation option utilisant "1-Second moniteur de performances »

Contenu

[Introduction](#)

[moniteur de performances 1-Second](#)

[Enable sur la version 5.4 ou ultérieures](#)

[Enable sur des versions antérieures à 5.4](#)

[Documents connexes](#)

Introduction

Sur une appliance exécutant le logiciel de Sourcefire, vous pouvez configurer les paramètres de base qui surveillent et rendent compte de sa propre représentation. La statistique de représentation est essentielle de dépanner des problèmes relatifs aux performances sur une exécution d'appareils reniflent. Ce document fournit les étapes pour activer cette caractéristique utilisant un centre de Gestion de FireSIGHT.

Avertissement : Si votre réseau est vivant et vous activez la représentation 1-Second sur un système de production, il peut affecter des performances du réseau. Vous devriez activer ceci seulement si ceci est demandé par le support technique de Cisco pour dépannage du but.

Remarque: 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).

moniteur de performances 1-Second

La caractéristique du *moniteur de performances 1-Second* te permet pour spécifier les intervalles auxquels le système met à jour des statistiques de représentation sur vos périphériques en configurant ce qui suit :

- Nombre de secondes
- Nombre de paquets analysés

Quand le nombre de secondes spécifiées s'est écoulé puisque la dernière mise à jour de statistiques de représentation, le système vérifie que le nombre spécifié de paquets a été analysé. Si oui, le système met à jour des statistiques de représentation. Sinon, le système attend jusqu'à ce que le nombre spécifié de paquets ait été analysé.

Enable sur la version 5.4 ou ultérieures

Étape 1 : **Stratégies > contrôle d'accès** choisis. La page de stratégie de contrôle d'accès paraît.

Étape 2 : Cliquez sur l'icône de *crayon* à côté de la stratégie de contrôle d'accès que vous voulez éditer.

Étape 3 : Sélectionnez l'onglet **Avancé**. La page de paramètres avancés de stratégie de contrôle d'accès paraît.

The screenshot shows the 'Default Access Control' configuration page. At the top, there are tabs for 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. Under 'Policies', there are sub-tabs for 'Access Control', 'Intrusion', 'Files', 'Network Discovery', and 'SSL'. The main heading is 'Default Access Control' with a sub-heading 'Enter a description'. Below this, there are five tabs: 'Rules', 'Targets', 'Security Intelligence', 'HTTP Responses', and 'Advanced'. The 'Advanced' tab is highlighted with a red border.

Étape 4 : Cliquez sur l'icône de *crayon* à côté des configurations de représentation.

The screenshot shows the 'Performance Settings' configuration page. The title is 'Performance Settings' with a pencil icon. Below the title, there are several settings:

Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default
Regular Expression - Recursion Limit	Default
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

The 'Performance Statistics - Sample Time (seconds)' row is highlighted with a red border.

Étape 5 : Sélectionnez l'onglet de **statistiques de représentation** dans la fenêtre externe qui apparaît. Modifiez la période d'échantillon ou le nombre minimal de paquets comme décrit ci-dessus.

The screenshot shows the 'Performance Settings' configuration page in a modal window. The title is 'Performance Settings' with a question mark and close icon. Below the title, there are four tabs: 'Pattern Matching Limits', 'Performance Statistics', 'Regular Expression Limits', and 'Intrusion Event Logging Limits'. The 'Performance Statistics' tab is selected. Below the tabs, there are two input fields:

Sample time (seconds)	300
Minimum number of packets	10000

The 'Sample time (seconds)' field is highlighted with a red border. Below the input fields, there is a 'Troubleshooting Options' section with a dropdown arrow. At the bottom of the modal, there are three buttons: 'Revert to Defaults', 'OK', and 'Cancel'.

Étape 6 : *Sur option*, développez la **section Options de dépannage** et modifiez ces options seulement si demandé de faire ainsi par Cisco TAC.

Étape 7 : Cliquez sur **OK**.

Étape 8 : Vous devez sauvegarder et appliquer la stratégie de contrôle d'accès pour que vos modifications les prennent effet.

Enable sur des versions antérieures à 5.4

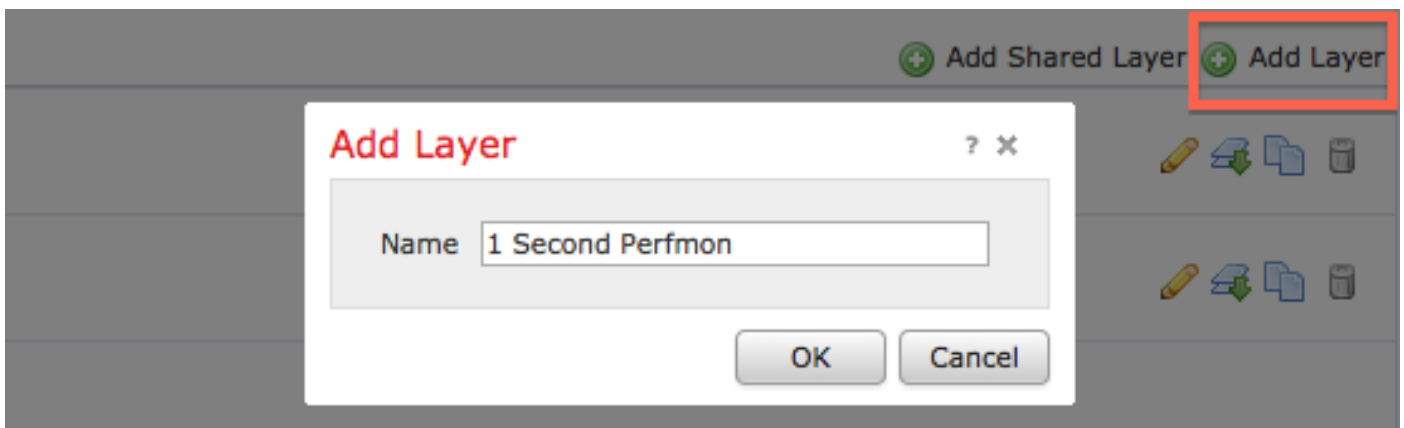
Étape 1 : Naviguez vers la page de stratégie d'intrusion. Procédure de connexion à votre centre de Gestion de FireSIGHT. Naviguez vers des **stratégies > l'intrusion > la stratégie d'intrusion**.

Étape 2 : Éditez la stratégie d'intrusion que vous voulez appliquer. Cliquez sur l'icône de *crayon* pour éditer la stratégie.

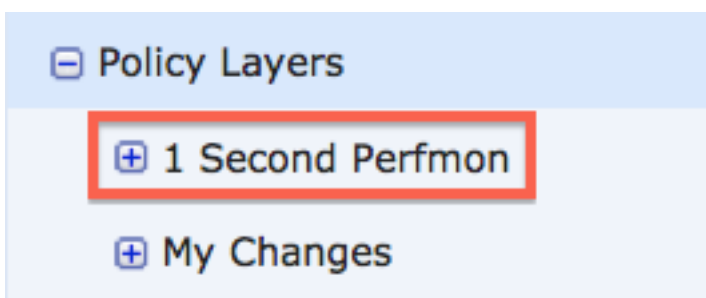


Remarque: En raison de la conception de ce paramètre avancé, vous devez seulement modifier cette configuration dans une stratégie d'intrusion qui est utilisée comme action par défaut de votre stratégie de contrôle d'accès.

Étape 3 : Ajoutez une couche de stratégie. Cliquez sur les **couches de stratégie** et puis **ajoutez la couche**. Nommez la couche le « *1 seconde Perfmon* ».









Vérifiez les **couches de stratégie** dans le panneau gauche, et assurez-vous que la nouvelle couche le « *1 seconde Perfmon* » est surtout d'autres couches.



Étape 4 : Activez la configuration de statistiques de représentation. Sous des **configurations de représentation**, sélectionnez la case d'option **activée** à côté de la **configuration de statistiques de représentation**, et cliquez sur Edit.

Performance Settings

Event Queue Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Latency-Based Packet Handling	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Latency-Based Rule Handling	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Performance Statistics Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Regular Expression Limits	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Rule Processing Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit

Étape 5 : Modifiez le temps par défaut d'échantillon à 1 seconde, et le nombre minimal de paquets à 100 paquets.

Performance Statistics Configuration

Settings

Sample time	<input type="text" value="1"/>	seconds
Minimum number of packets	<input type="text" value="100"/>	

Étape 6 : Cliquez sur en fonction les **informations de stratégie** dans le panneau gauche, commettez les modifications, et appliquez la stratégie mise à jour aux périphériques que vous voudriez profiler.

Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings

Étape 7 : Retournez les configurations après avoir collecté les données. Afin de retourner, supprimez simplement la couche de stratégie du « 1 seconde Perfmon ».

Attention : N'oubliez pas de retourner la configuration. Autrement, il peut entraîner le problème de performance.

Documents connexes

- [Visionnement de la représentation d'événement d'intrusion](#)
- [Générer des graphiques de statistiques de représentation d'événement d'intrusion](#)