

「1-Second Performance Monitor」オプションを使用したパフォーマンス統計情報の収集

内容

[概要](#)

[1秒パフォーマンスモニタ](#)

[バージョン5.4以降で有効にする](#)

[5.4より前のバージョンで有効にする](#)

[関連資料](#)

概要

Sourcefire ソフトウェアが動作するアプライアンスでは、各自のパフォーマンスをモニタおよび報告する基本パラメータを設定できます。パフォーマンス統計情報は、Snort が動作するアプライアンスでパフォーマンス関連の問題をトラブルシューティングする際に重要です。このドキュメントでは、FireSIGHT Management Center を使用してこの機能を有効にする手順を説明します。

警告： ネットワークが稼働中で、実稼働システムで1秒のパフォーマンスを有効にすると、ネットワークのパフォーマンスに影響する可能性があります。これは、トラブルシューティングのためにシスコテクニカルサポートから要求された場合にのみ有効にしてください。

注： このドキュメントの情報は、特定のラボ環境のデバイスから作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。

1秒パフォーマンスモニタ

1-Second Performance Monitor 機能を使用すると、次の設定を行うことで、デバイスのパフォーマンス統計情報をシステムが更新する間隔を指定できます。

- 秒数
- 分析されたパケット数

最後のパフォーマンス統計情報の更新以降に指定した秒数が経過すると、システムは指定した数のパケットが分析されたことを確認します。その場合、システムはパフォーマンス統計情報を更新します。そうでない場合、システムは指定された数のパケットが分析されるまで待機します。

バージョン5.4以降で有効にする

ステップ 1 : [Policies] > [Access Control]を選択します。[Access Control Policy]ページが表示されます。

ステップ 2 : 編集するアクセス制御ポリシーの横にある鉛筆アイコンをクリックします。

ステップ 3 : [Advanced] タブを選択します。アクセスコントロールポリシーの詳細設定ページが表示されます。

Overview Analysis **Policies** Devices Objects AMP

Access Control Intrusion ▾ Files Network Discovery SSL

Default Access Control

Enter a description

Rules Targets Security Intelligence HTTP Responses **Advanced**

ステップ 4 : [パフォーマンス設定]の横にある鉛筆アイコンをクリックします。

Performance 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

ステップ 5 : 表示されるポップアップ・ウィンドウで[パフォーマンス統計]タブを選択します。上記のように、[Sample time]または[Minimum number of packets]を変更します。

Performance Settings ? ×

Pattern Matching Limits **Performance Statistics** Regular Expression Limits Intrusion Event Logging Limits

Sample time (seconds)	300
Minimum number of packets	10000

Troubleshooting Options ▾

Revert to Defaults OK Cancel

ステップ 6 : 必要に応じて、[Troubleshoot Options]セクションを展開し、Cisco TACに依頼された場合にのみ、これらのオプションを変更します。

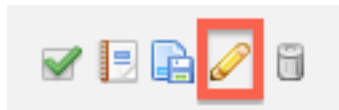
手順 7 : [OK] をクリックします。

ステップ 8 : 変更を有効にするには、アクセスコントロールポリシーを保存して適用する必要があります。

5.4より前のバージョンで有効にする

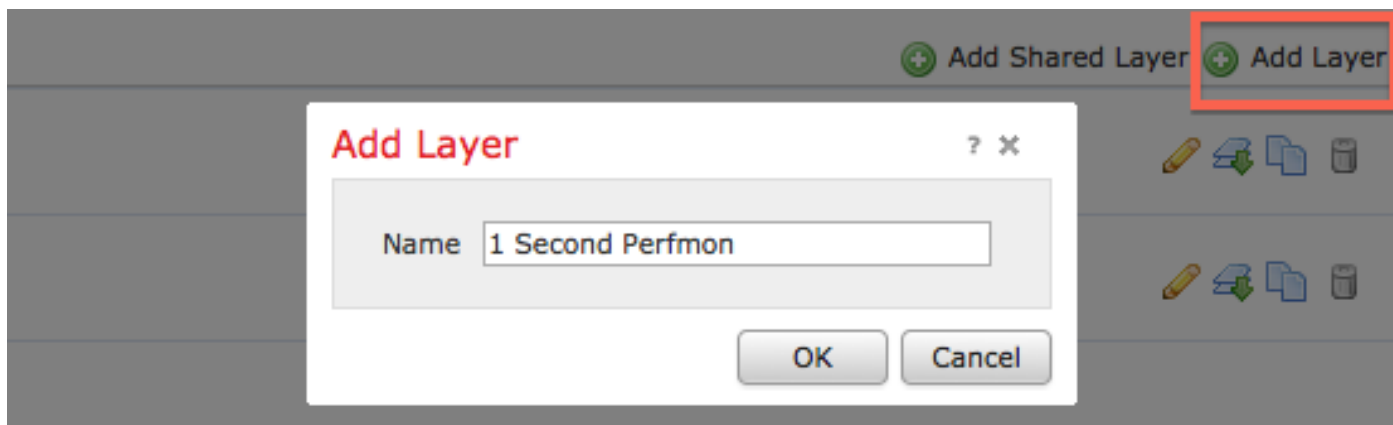
ステップ 1 : [Intrusion Policy]ページに移動します。FireSIGHT Management Centerにログインします。[Policies] > [Intrusion] > [Intrusion Policy] に移動します。

ステップ 2 : 適用する侵入ポリシーを編集します。鉛筆アイコンをクリックして、ポリシーを編集します。

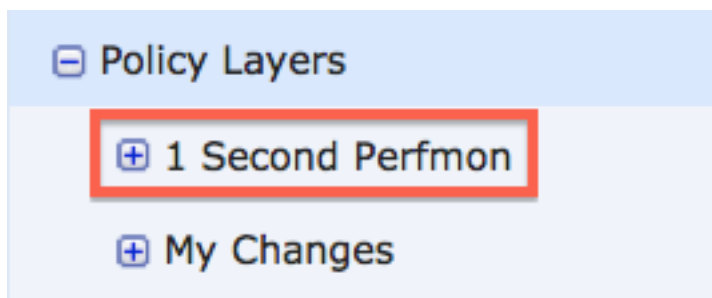


注 : この詳細設定の設計により、アクセスコントロールポリシーのデフォルトアクションとして使用されている侵入ポリシー内でこの設定を変更する必要があります。

ステップ 3 : ポリシーレイヤを追加します。[Policy Layers]をクリックし、[Add Layer]をクリックします。レイヤに「1 Second Perfmon」という名前を付けます。









左側のパネルの[Policy Layers]をチェックし、新しいレイヤ「1 Second Perfmon」が他のすべてのレイヤの上に配置されていることを確認してください。



ステップ 4 : パフォーマンス統計情報の設定を有効にします。[パフォーマンス設定]で、[パフォーマンス統計の構成]の横にある[有効]ラジオボタンをオンに選択し、[編集]をクリックします。

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

ステップ 5 : デフォルトのサンプル時間を1秒に、最小パケット数を100パケットに変更します。

Performance Statistics Configuration

Settings

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

ステップ 6 : 左側のパネルの[Policy Information]をクリックし、変更を確定し、更新したポリシーをプロファイルするデバイスに適用します。

Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings

手順 7 : データ収集後に設定を元に戻します。元に戻すには、「1 Second Perfmon」ポリシー層を削除するだけです。

注意 : 設定を元に戻すことを忘れないでください。そうしないと、パフォーマンスの問題が発生する可能性があります。

関連資料

- [侵入イベントパフォーマンスの表示](#)
- [侵入イベントパフォーマンス統計グラフの生成](#)