

# Coleta de estatísticas de desempenho usando a opção "Monitor de desempenho de 1 segundo"

## Contents

[Introduction](#)

[Monitor de desempenho de 1 segundo](#)

[Ativar na versão 5.4 ou posterior](#)

[Ativar versões anteriores à 5.4](#)

[Documentos relacionados](#)

## Introduction

Em um dispositivo que executa o software Sourcefire, você pode configurar os parâmetros básicos que monitoram e relatam seu próprio desempenho. A estatística de desempenho é essencial para solucionar problemas relacionados ao desempenho em um dispositivo que executa o Snort. Este documento fornece as etapas para habilitar esse recurso usando um FireSIGHT Management Center.

**Aviso:** se sua rede estiver ativa e você habilitar o desempenho de 1 segundo em um sistema de produção, isso poderá afetar o desempenho da rede. Você deve habilitá-lo apenas se isso for solicitado pelo Suporte Técnico da Cisco para fins de solução de problemas.

**Observação:** as informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration.

## Monitor de desempenho de 1 segundo

O recurso *Monitor de Desempenho de 1 Segundo* permite especificar os intervalos nos quais o sistema atualiza as estatísticas de desempenho em seus dispositivos configurando o seguinte:

- Número de segundos
- Número de pacotes analisados

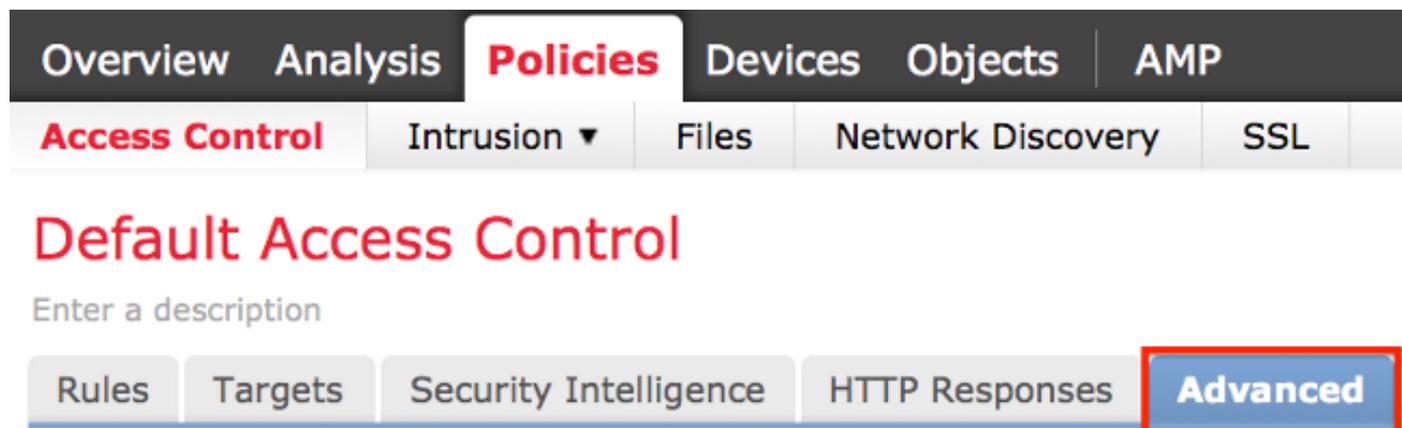
Quando o número de segundos especificado tiver decorrido desde a última atualização de estatísticas de desempenho, o sistema verificará se o número especificado de pacotes foi analisado. Em caso afirmativo, o sistema atualiza as estatísticas de desempenho. Caso contrário, o sistema espera até que o número especificado de pacotes seja analisado.

## Ativar na versão 5.4 ou posterior

**Passo 1:** Selecione **Políticas > Controle de acesso**. A página Access Control Policy (Política de controle de acesso) é exibida.

**Passo 2:** Clique no ícone *lápis* ao lado da diretiva de controle de acesso que deseja editar.

**Passo 3:** Selecione a guia Advanced. A página de configurações avançadas da política de controle de acesso é exibida.



The screenshot shows the Cisco AMP interface. At the top, there is a navigation bar with tabs: Overview, Analysis, **Policies**, Devices, Objects, and AMP. Below this, there is a sub-navigation bar with tabs: **Access Control**, Intrusion, Files, Network Discovery, and SSL. The main content area is titled 'Default Access Control' and has a text input field 'Enter a description'. Below the input field, there is a row of sub-tabs: Rules, Targets, Security Intelligence, HTTP Responses, and **Advanced** (which is highlighted with a red box).

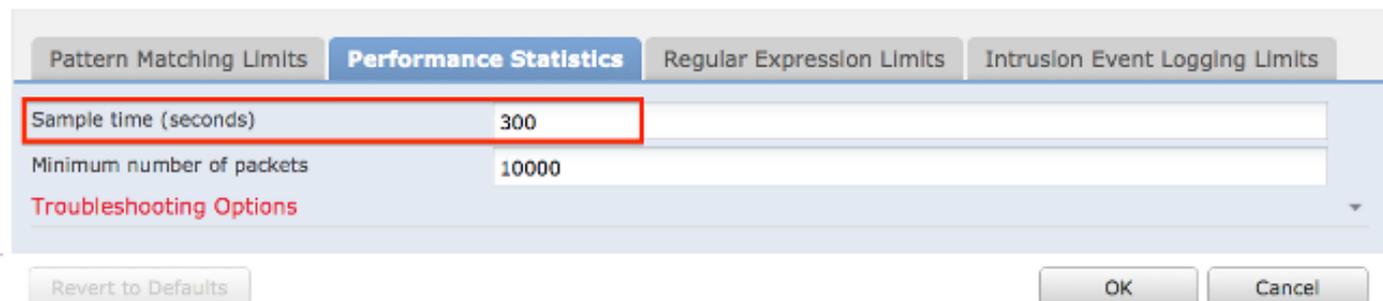
**Passo 4:** Clique no ícone *do lápis* ao lado de **Configurações de desempenho**.

### Performance Settings

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

**Passo 5:** Selecione a guia **Estatísticas de desempenho** na janela pop-up exibida. Modifique o tempo de exemplo ou o número mínimo de pacotes conforme descrito acima.

### Performance Settings



The screenshot shows a dialog box titled 'Performance Settings' with a close button (X) and a help button (?). It has four tabs: Pattern Matching Limits, **Performance Statistics**, Regular Expression Limits, and Intrusion Event Logging Limits. The 'Performance Statistics' tab is active. It contains two input fields: 'Sample time (seconds)' with the value '300' (highlighted with a red box) and 'Minimum number of packets' with the value '10000'. Below the input fields is a section for 'Troubleshooting Options'. At the bottom of the dialog, there are three buttons: 'Revert to Defaults', 'OK', and 'Cancel'.

**Passo 6:** *Opcionalmente*, expanda a seção **Solucionar problemas** e modifique essas opções somente se solicitado pelo Cisco TAC.

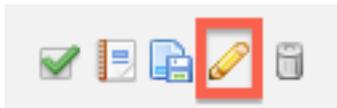
**Passo 7:** Click OK.

**Passo 8:** Você deve salvar e aplicar a política de controle de acesso para que as alterações entrem em vigor.

## Ativar versões anteriores à 5.4

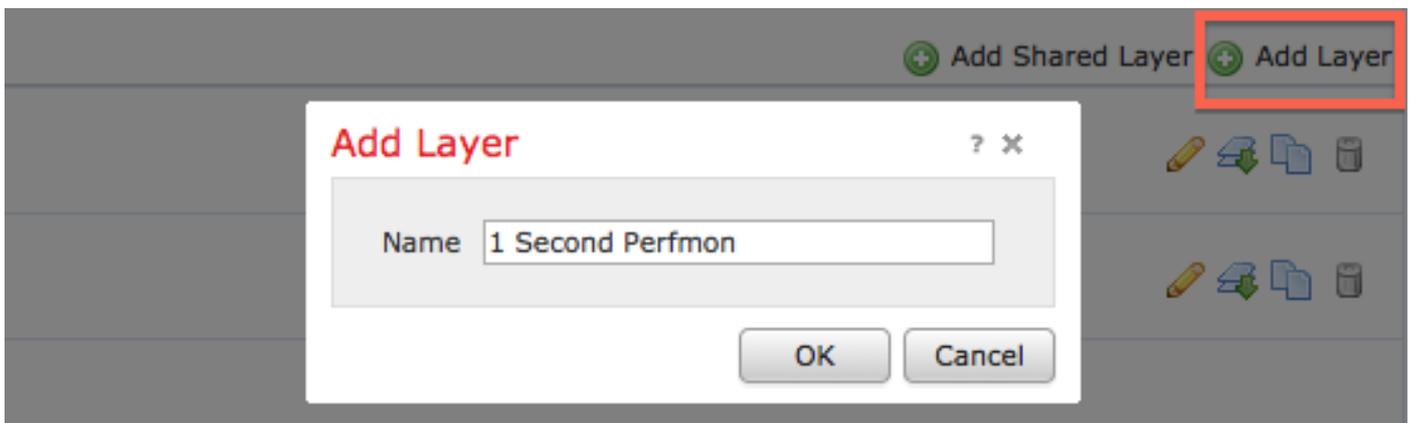
**Passo 1:** Navegue até a página Política de intrusão. Faça login no FireSIGHT Management Center. Navegue até **Políticas > Intrusion > Intrusion Policy (Políticas > Intrusion > Política de intrusão)**.

**Passo 2:** Edite a política de intrusão que deseja aplicar. Clique no ícone *do lápis* para editar a diretiva.

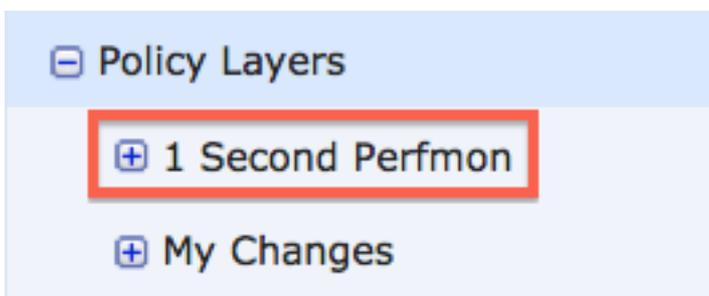


**Note:** Devido ao projeto dessa configuração avançada, você deve modificar essa configuração somente em uma Política de intrusão que está sendo usada como a ação padrão da sua Política de controle de acesso.

**Passo 3:** Adicione uma camada de política. Clique em **Camadas de política** e em **Adicionar camada**. Nomeie a camada "*1 Second Perfmon*".



Verifique as **Camadas de política** no painel esquerdo e certifique-se de que a nova camada "*1 Segundo Perfmon*" esteja acima de todas as outras camadas.



**Passo 4:** Ative a configuração de estatísticas de desempenho. Em **Configurações de desempenho**, selecione o botão de opção **Habilitado** ao lado da **Configuração de estatísticas de desempenho** e clique em **Editar**.

## 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

**Passo 5:** Modifique o tempo de amostra padrão para 1 segundo e o número mínimo de pacotes para 100 pacotes.

### Performance Statistics Configuration

#### Settings

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

**Passo 6:** Clique em **Policy Information (Informações da política)** no painel esquerdo, confirme as alterações e aplique a política atualizada aos dispositivos que você gostaria de criar o perfil.

### Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings

**Passo 7:** Reverta as configurações após coletar os dados. Para reverter, simplesmente exclua a camada de política "1 Segundo Perfmon".

**Caution:** Não se esqueça de reverter a configuração. Caso contrário, pode causar

problemas de desempenho.

## Documentos relacionados

- [Visualizando o desempenho do evento de intrusão](#)
- [Gerando Gráficos de Estatísticas de Desempenho de Eventos de Invasão](#)