

Coleção das estatísticas de desempenho usando opção do monitoramento de desempenho "1-Second"

Índice

[Introdução](#)

[monitoramento de desempenho 1-Second](#)

[Permita na versão 5.4 ou mais recente](#)

[Permita em versões antes de 5.4](#)

[Documentos relacionados](#)

Introdução

Em um dispositivo que executa o software de Sourcefire, você pode configurar os parâmetros básicos que monitor e relatório em seu próprio desempenho. A estatística de desempenho é crítica para pesquisar defeitos questões relacionadas ao desempenho em um Snort do corredor do dispositivo. Este documento fornece as etapas para permitir esta característica usando um centro de gerenciamento de FireSIGHT.

aviso: Se sua rede está viva e você permite o desempenho 1-Second em um sistema da produção, pode impactar o desempenho da rede. Você deve permitir este somente se este é pedido pelo Suporte técnico de Cisco para o propósito de Troubleshooting.

Note: As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial.

monitoramento de desempenho 1-Second

A característica do *monitoramento de desempenho 1-Second* permite que você especifique os intervalos em que as estatísticas de desempenho das atualizações de sistema em seus dispositivos configurando o seguinte:

- Número de segundos
- Número de pacotes analisados

Quando o número de segundos especificados decorrer desde que a última atualização das estatísticas de desempenho, o sistema verifica que o número especificado de pacotes esteve analisado. Em caso afirmativo, as estatísticas de desempenho das atualizações de sistema. Se

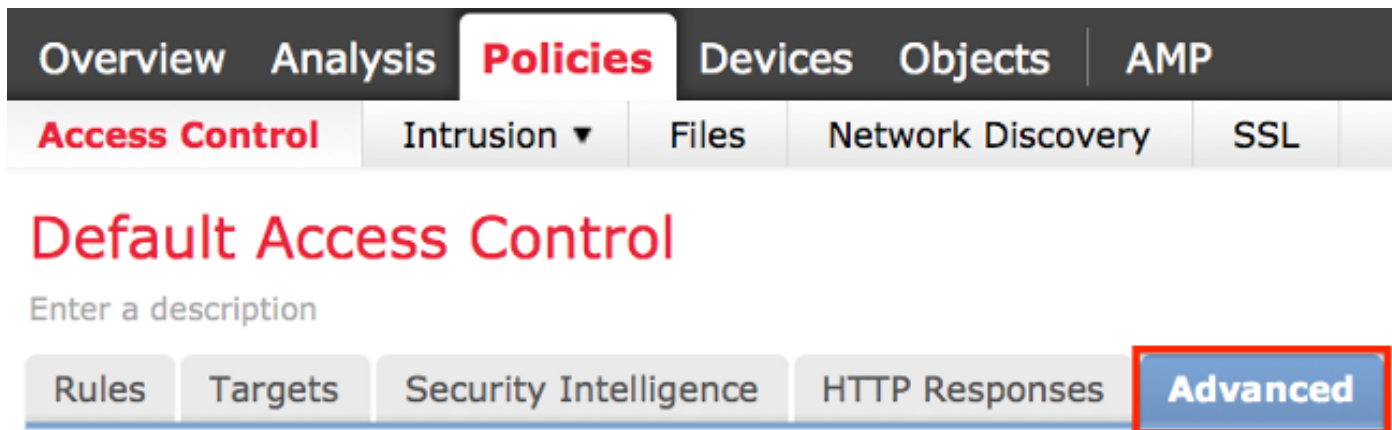
não, as esperas do sistema até o número especificado de pacotes foram analisadas.

Permita na versão 5.4 ou mais recente

Passo 1: Selecione **políticas > controle de acesso**. A página da política do controle de acesso publica-se.

Passo 2: Clique o ícone do *lápiz* ao lado da política que do controle de acesso você quer editar.

Passo 3: Selecione a guia Advanced. A página avançada política dos ajustes do controle de acesso publica-se.



The screenshot shows the Cisco ASA configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. Below this, there are sub-tabs for 'Access Control', 'Intrusion', 'Files', 'Network Discovery', and 'SSL'. The main heading is 'Default Access Control'. Below the heading is a text input field 'Enter a description'. At the bottom, there are five sub-tabs: 'Rules', 'Targets', 'Security Intelligence', 'HTTP Responses', and 'Advanced'. The 'Advanced' tab is highlighted with a red box.

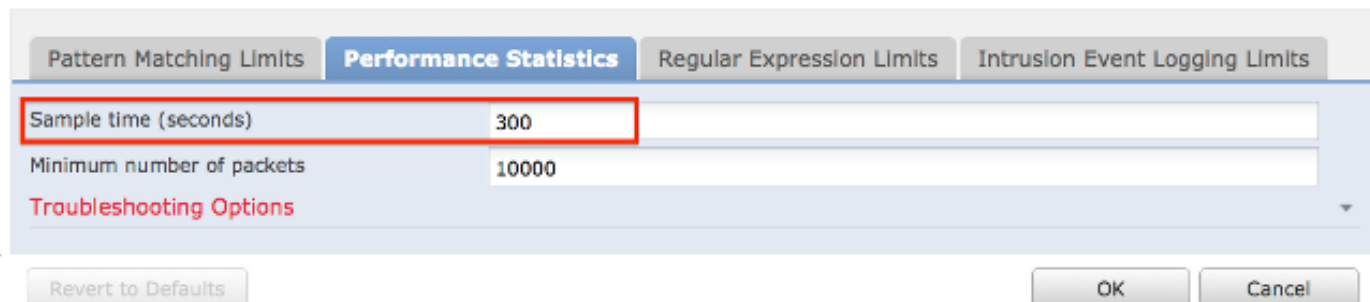
Passo 4: Clique o ícone do *lápiz* ao lado dos **ajustes do desempenho**.

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

Passo 5: Selecione a aba das **estatísticas de desempenho** na janela pop-up que aparece. Altere a época da amostra ou o número mínimo de pacotes como descrito acima.

Performance Settings



The screenshot shows a pop-up window titled 'Performance Settings'. It has 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)' with a value of 300, and 'Minimum number of packets' with a value of 10000. Below these fields is a section for 'Troubleshooting Options'. At the bottom of the window, there are three buttons: 'Revert to Defaults', 'OK', and 'Cancel'.

Passo 6: *Opcionalmente*, expanda a seção das **opções da pesquisa de defeitos** e altere aquelas opções somente se perguntado fazer assim pelo tac Cisco.

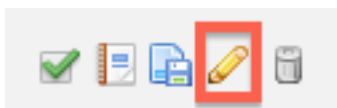
Passo 7: Clique em OK.

Passo 8: Você deve salvar e aplicar a política do controle de acesso para que suas mudanças tomem o efeito.

Permita em versões antes de 5.4

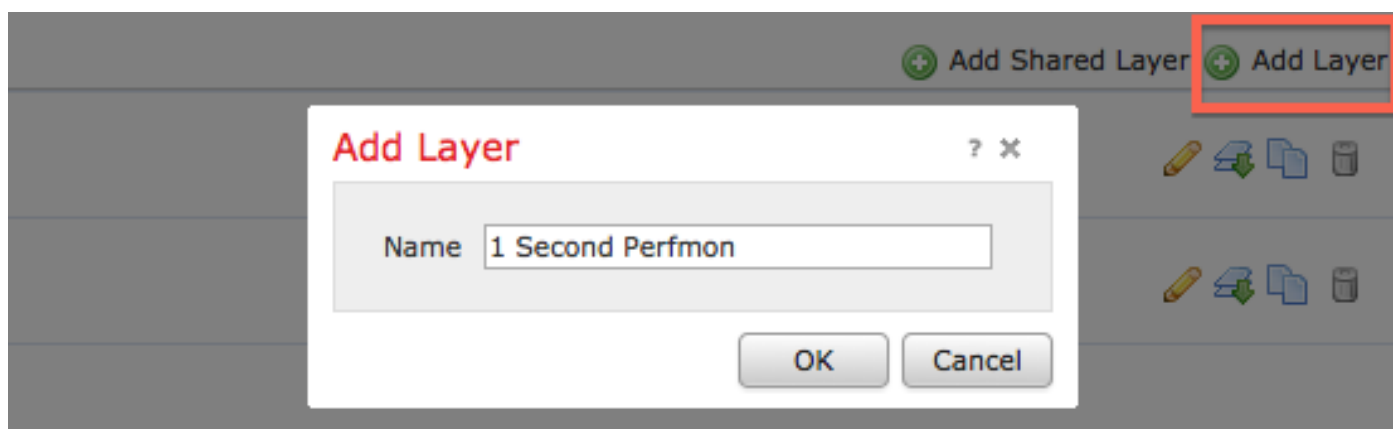
Passo 1: Navegue à página da política da intrusão. Entre a seu centro de gerenciamento de FireSIGHT. Navegue às **políticas > à intrusão > à política da intrusão**.

Passo 2: Edite a política da intrusão que você quer aplicar. Clique o ícone do *lápiz* para editar a política.

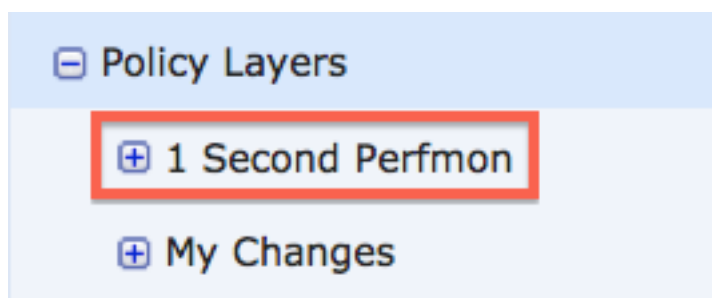


Note: Devido ao projeto deste ajuste avançado, você deve somente alterar esta configuração dentro de uma política da intrusão que esteja sendo usada como a ação padrão de sua política do controle de acesso.

Passo 3: Adicionar uma camada da política. Clique **camadas da política** e **adicionar** então a **camada**. Nomeie a camada “*1 segundo perfmon*”.









Verifique as **camadas da política** no painel esquerdo, e certifique-se de que a camada nova “*1 segundo perfmon*” é sobretudo outras camadas.



Passo 4: Permita a configuração das estatísticas de desempenho. Sob **ajustes do desempenho**, selecione o botão de rádio **permitido** ao lado da **configuração das estatísticas de desempenho**, e o clique **edita**.

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: Altere o tempo da amostra do padrão a 1 segundo, e o número mínimo de pacotes a 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 sobre a **informação sobre a política** no painel esquerdo, comprometa as mudanças, e aplique a política actualizado aos dispositivos que você gostaria de perfilar.

Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings

Passo 7: Reverta os ajustes após ter recolhido os dados. A fim reverter, suprima simplesmente de “da camada da política *1 segundo perfmon*”.

Caution: Não esqueça reverter a configuração. Se não, pode causar o problema de

desempenho.

Documentos relacionados

- [Vendo o desempenho do evento da intrusão](#)
- [Gerando gráficos das estatísticas de desempenho do evento da intrusão](#)