

Набор статистики производительности Использование "1-секундного монитора производительности" опция

Содержание

[Введение](#)

[1-секундный монитор производительности](#)

[Включите на версии 5.4 или позже](#)

[Включите на версиях до 5.4](#)

[Дополнительная документация](#)

Введение

На устройстве, выполняющем программное обеспечение Sourcefire, можно настроить основные параметры, которые отслеживают и сообщают на его собственной производительности. Статистика производительности важна для устранения проблем связанных с производительностью проблема на Фырканые выполнения устройства. Этот документ предоставляет шаги для включения этой опции с помощью Центра управления FireSIGHT.

% Warning: Если ваша сеть является оперативной, и вы включаете 1--секундную Производительность на производственной системе, это может повлиять на производительность сети. Необходимо включить это, только если это запрашивает техническая поддержка Cisco на цель устранения проблем.

Примечание: Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию.

1-секундный монитор производительности

1-секундная функция *Монитора производительности* позволяет вам задавать интервалы в который статистика производительности обновлений системы на ваших устройствах путем настройки придерживающегося:

- Кол-во секунд
- Количество пакетов проанализировано

Когда заданное кол-во секунд истекло начиная с последнего обновления статистики

производительности система проверяет, что был проанализирован заданный номер пакетов. Если так, статистика производительности обновлений системы. В противном случае система ждет, пока заданный номер пакетов не был проанализирован.

Включите на версии 5.4 или позже

Шаг 1: Выберите **Policies > Access Control**. Страница Access Control Policy появляется.

Шаг 2: Нажмите *значок карандаша* рядом с политикой контроля доступа, которую вы хотите отредактировать.

Шаг 3: Откройте вкладку **Advanced (Дополнительно)**. Страница расширенных настроек политики контроля доступа появляется.

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**

Шаг 4. : Нажмите *значок карандаша*, следующий за **Параметрами настройки Производительности**.

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

Шаг 5. : Выберите вкладку **Performance Statistics** во всплывающем окне, которое появляется. Модифицируйте Типовое время или Минимальное количество пакетов, как описано выше.

Performance Settings ? x

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

Шаг 6: Дополнительно, разверните раздел **Опций Устранения неполадок** и модифицируйте те опции только если попросивший сделать так Центром технической поддержки Cisco.

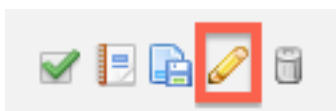
Шаг 7 Нажмите ОК.

Шаг 8: Необходимо сохранить и применить политику контроля доступа для изменений для вступления в силу.

Включите на версиях до 5.4

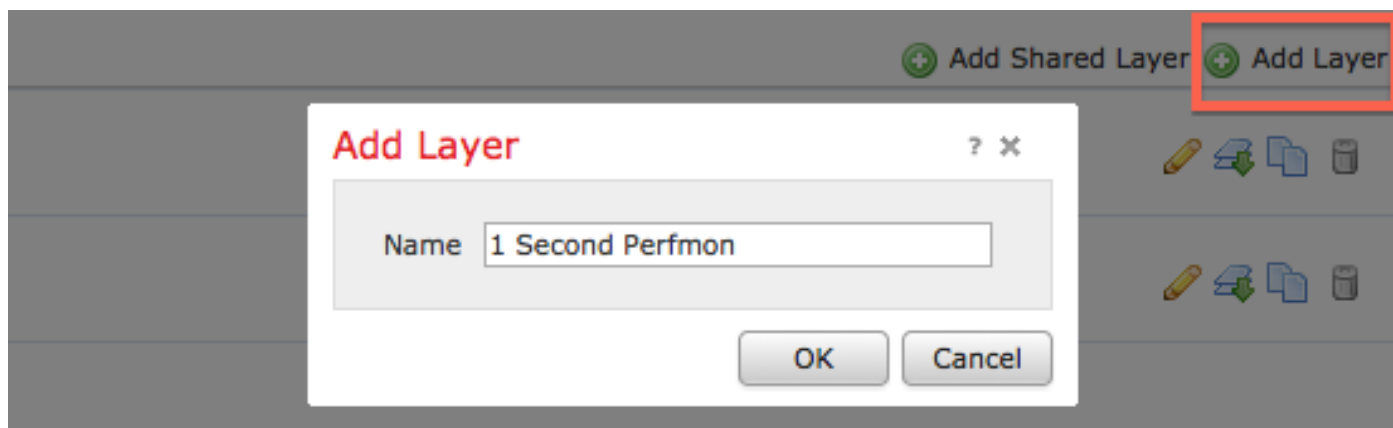
Шаг 1: Перейдите к странице Policy Проникновения. Вход в систему к вашему Центру управления FireSIGHT. Перейдите к **Политике> Проникновение> Политика Проникновения**.

Шаг 2: Отредактируйте политику проникновения, которую вы хотите применить. Нажмите значок *карандаша* для редактирования политики.

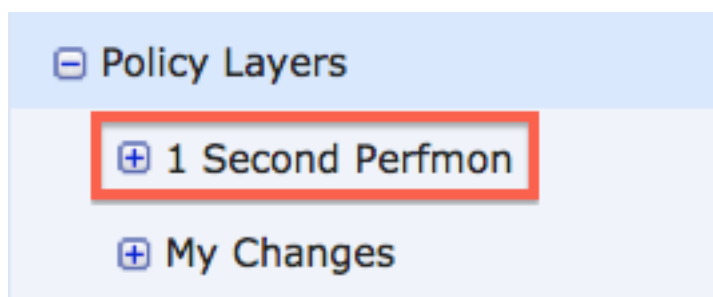


Примечание: Из-за дизайна этой расширенной настройки, необходимо только модифицировать эту конфигурацию в Политике Проникновения, которая используется в качестве Действия по умолчанию Политики контроля доступа.

Шаг 3: Добавьте уровень политики. Нажмите **Policy Layers** и затем **Добавьте Уровень**. Назовите уровень "**1 Вторым Perfmon**".



Проверьте **Уровни Политики** в левой панели и удостоверьтесь, что новый уровень "**1 Второй Perfmon**" является, прежде всего, другими уровнями.



Шаг 4. : Включите конфигурацию статистики производительности. При **Параметрах**

настройки Производительности выберите кнопку с зависимой фиксацией Enabled рядом с Конфигурацией Статистики производительности и нажмите 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

Шаг 5. : Модифицируйте типовое время по умолчанию к 1 секунде, и минимальный номер пакетов к 100 пакетам.

Performance Statistics Configuration

Settings

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

Шаг 6: Щелкните по **Policy Information** в левой панели, передайте изменения и примените обновленную политику к устройствам, которые требуется представить.

Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings

Шаг 7: Верните параметры настройки после сбора данных. Для возвращения просто

удалите "1 Второй Perfmon" уровень политики.

Внимание. : Не забывайте возвращать конфигурация. В противном случае это может вызвать проблему производительности.

Дополнительная документация

- [Просмотр производительности события проникновения](#)
- [Генерация графиков статистики производительности события проникновения](#)