Настройте систему FireSIGHT для передачи предупреждений к внешнему серверу системного журнала

Содержание

Введение

В то время как Система FireSIGHT предоставляет различные представления событий в, он - веб-интерфейс, можно хотеть настроить уведомление внешнего события для упрощения постоянного контроля Критических систем. Можно настроить Систему FireSIGHT для генерации предупреждений, которые уведомляют вас по электронной почте, trap-сообщение SNMP или системный журнал, когда один из ниже приводится генерируемый. Эта статья описывает, как настроить Центр управления FireSIGHT для передачи предупреждений на внешнем сервере системного журнала.

Предварительные условия

Требования

Cisco рекомендует ознакомиться на Центре управления Системного журнала и FireSIGHT. Кроме того, порт системного журнала (по умолчанию 514) должен быть позволен в вашем межсетевом экране.

Используемые компоненты

Сведения в этом документе основываются на Версии программного обеспечения 5.2 или позже.

Внимание. : Информация об этом документе создана от устройства в специальной лабораторной среде и запустила с чистой (заданной по умолчанию) конфигурацией. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Передача предупреждений проникновения

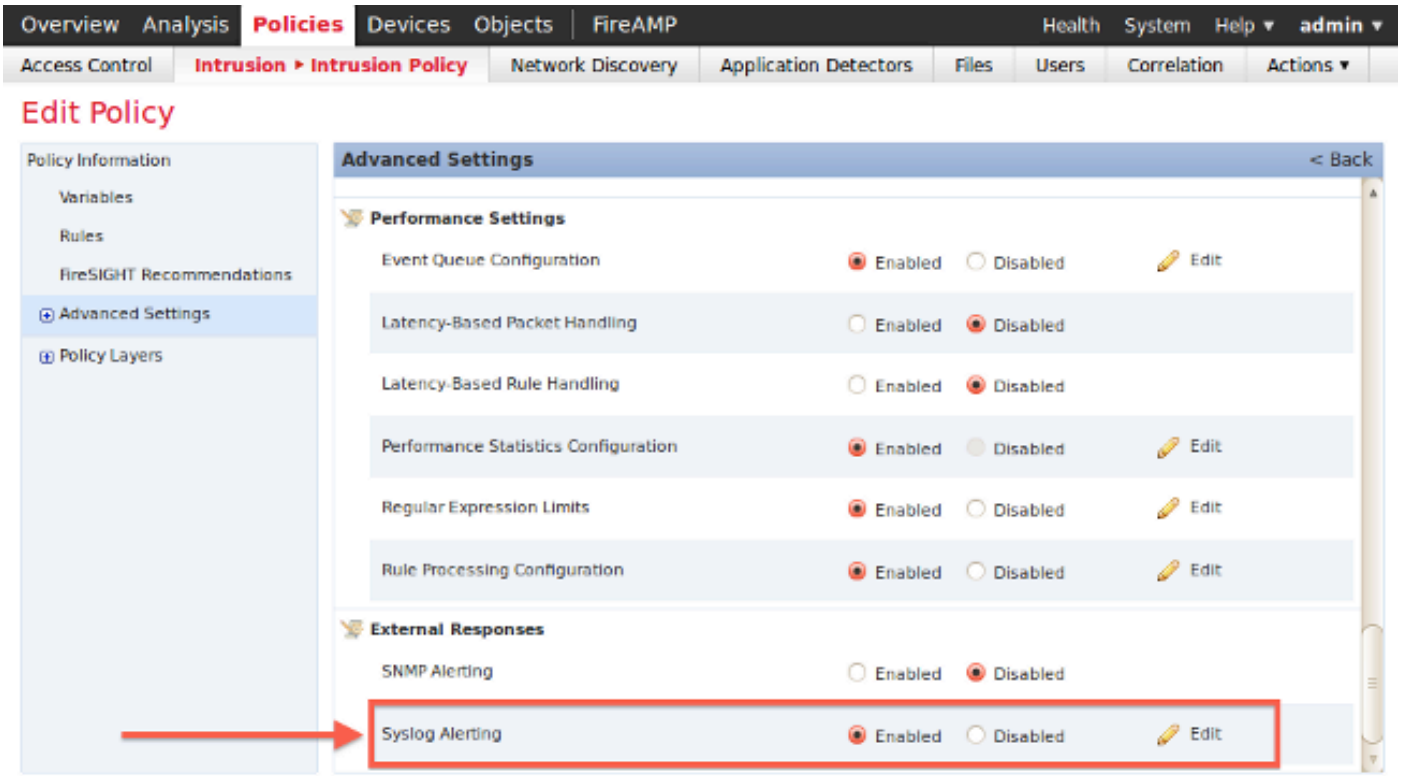
1. Войдите в интерфейс веба - пользователя своего Центра управления FireSIGHT.

2. Перейдите к **Политике> Проникновение> Политика Проникновения**.

3. Нажмите **Edit** рядом с политикой, которую вы хотите применить.

4. Щелкните **по Advanced Settings**.

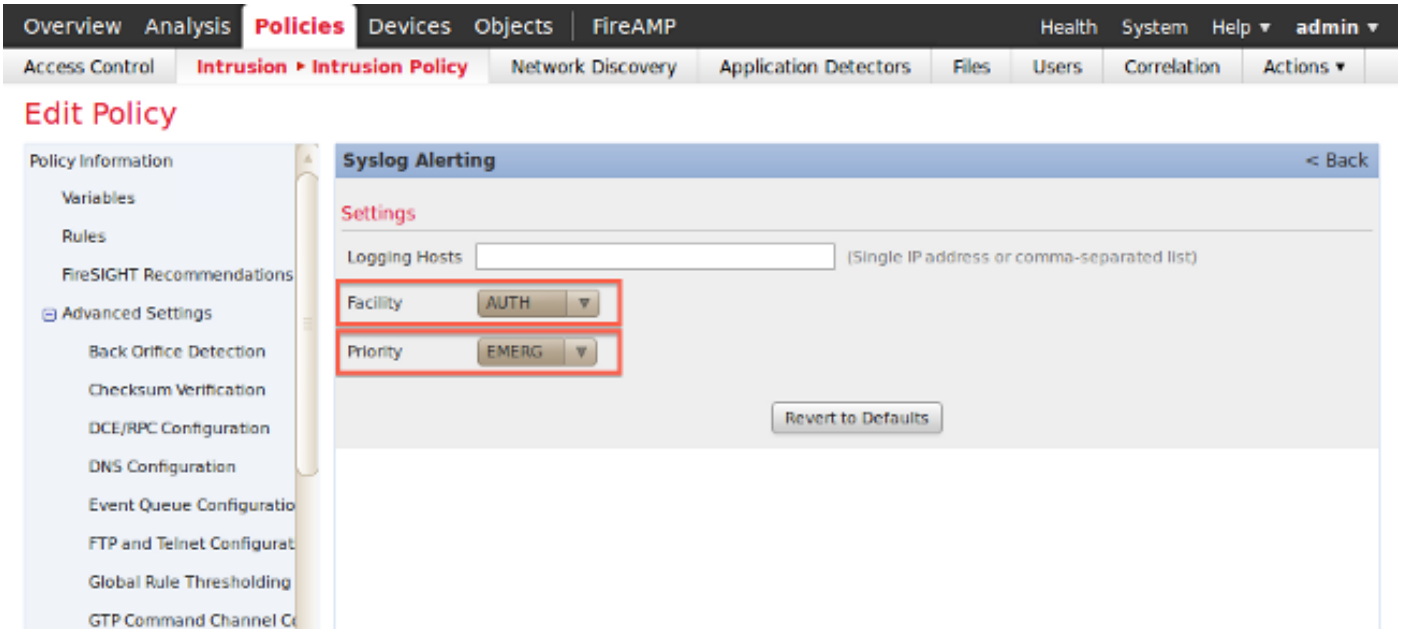
5. Найдите **Предупреждение Системного журнала** в списке и установите его во **Включенный**.



6. Нажмите **Edit** рядом с правом на **Предупреждение Системного журнала**.

7. Введите IP-адрес своего сервера системного журнала на поле **Logging Hosts**.

8. Выберите соответствующее **Средство** и **Степени серьезности ошибки** от раскрывающегося меню. Их можно оставить в значениях по умолчанию, пока сервер системного журнала не настроен для принятия предупреждений для определенного средства или степеней серьезности ошибки.



9. Щелкните **по Policy Information** около левого верхнего из этого экрана.

10. Нажмите кнопку **Commit Changes**.

11. Повторно примените свою политику проникновения.

> **Примечание:** Для предупреждений, которые будут генерироваться, используйте эту политику проникновения в правиле Управления доступом. Если нет никакого настроенного правила Управления доступом, то установленный эта политика проникновения, которая будет использоваться в качестве действия по умолчанию Политики контроля доступа, и повторно применяет Политику контроля доступа.

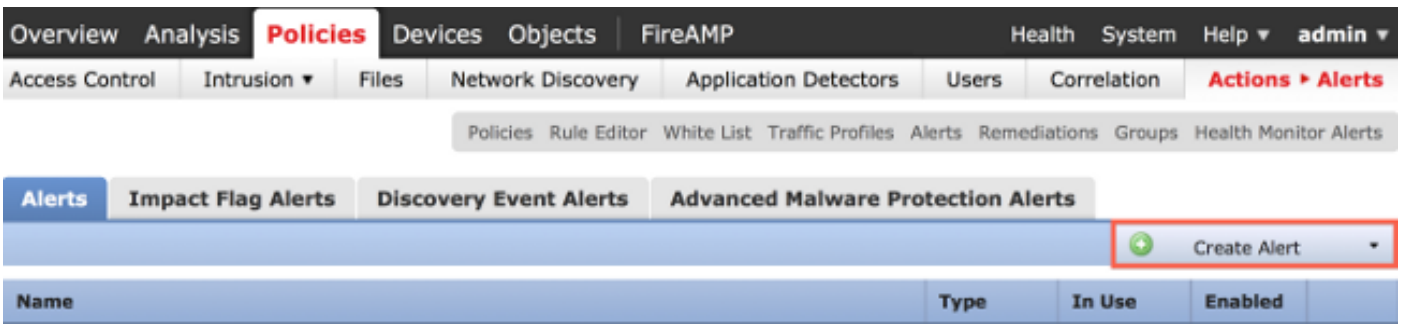
Теперь, если событие проникновения включено, что политика, предупреждение будет также передаваться серверу системного журнала, который настроен на политике проникновения.

Передача предупреждений состояния

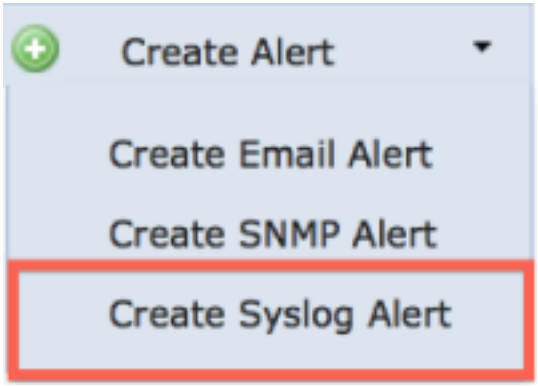
Часть 1: создайте предупреждение системного журнала

1. Войдите в интерфейс веба - пользователя своего Центра управления FireSIGHT.

2. Перейдите к **Политике> Действия> Предупреждения**.



3. Выберите **Create Alert**, который имеет на правой стороне веб-интерфейс.



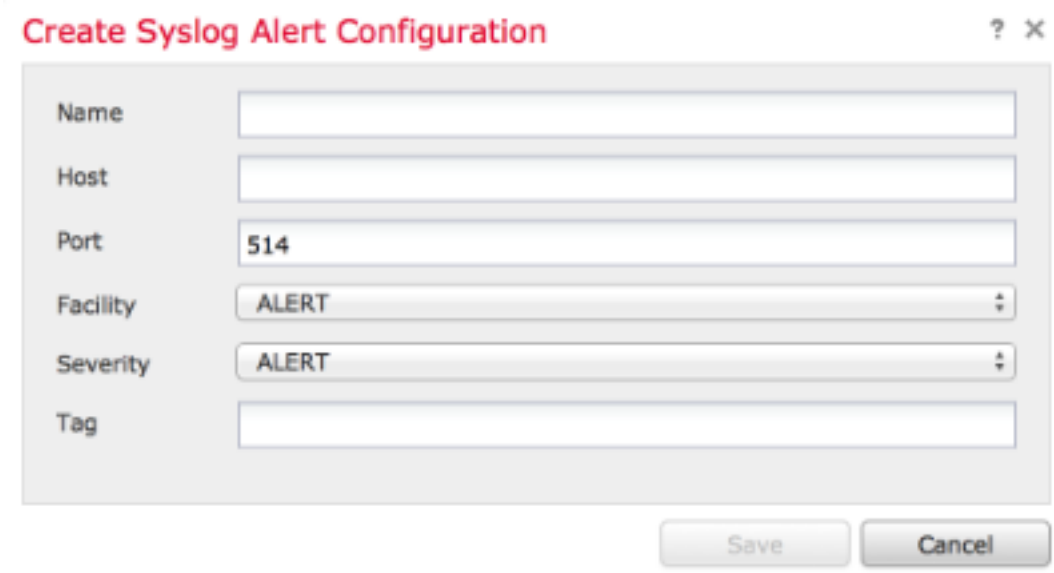
4. Нажмите **Create Syslog Alert**. Всплывающее окно конфигурации появляется.

5. Предоставьте название для предупреждения.

6. Заполните IP-адрес своего сервера системного журнала в **поле Host**.

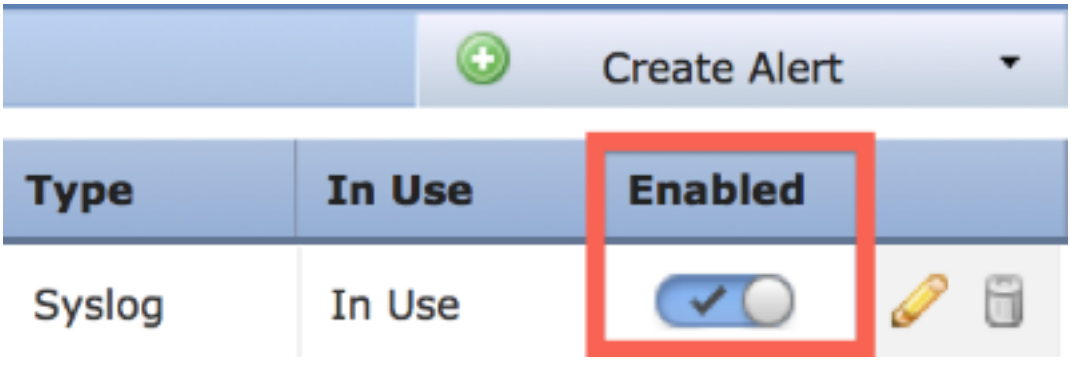
7. Измените порт в случае необходимости вашим сервером системного журнала (порт по умолчанию 514).

8. Выберите соответствующее **Средство** и **Степени серьезности ошибки**.



9. **Нажать кнопку Save (сохранить)**. Вы возвратитесь к странице **Policies> Actions> Alerts**.

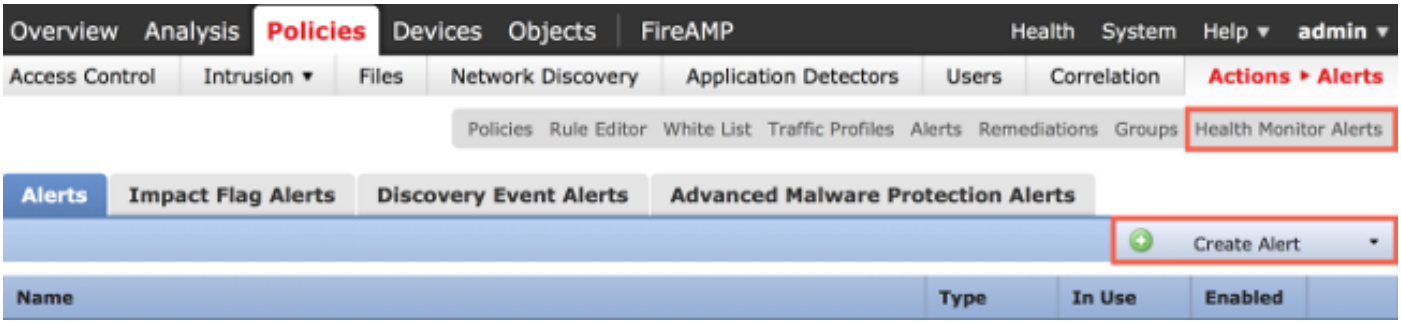
10. Включите Конфигурацию системного журнала.



Часть 2: создайте предупреждения контроля исправности

Следующие инструкции описывают шаги для настройки **Предупреждений Контроля исправности**, который использует предупреждение системного журнала, что вы только что создали (в предыдущем разделе):

1. Перейдите к странице **Policies> Actions> Alerts** и выберите **Health Monitor Alerts**, который является около начала страницы.



2. Дайте предупреждению состояния название.

3. Выберите **Severity** (удержание клавиши CTRL, в то время как нажатие может использоваться для выбора нескольких типов степени серьезности).

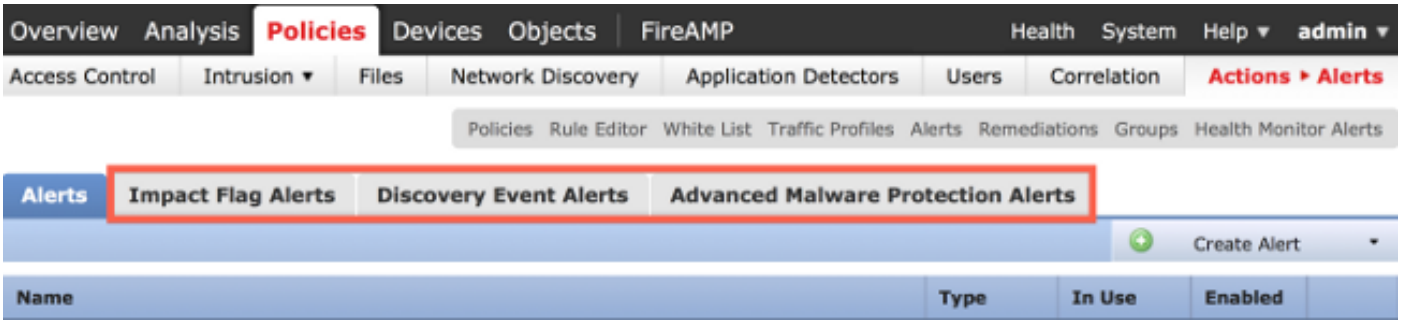
4. От **Модуля** columnm выбирают модули состояния, для которых требуется передать предупреждения к серверу системного журнала (Например, Использование диска).

5. Выберите созданное на предыдущем этапе предупреждение системного журнала от столбца **Alerts**.

6. **Нажать кнопку Save (сохранить).**

При передаче флага влияния обнаружьте событие и вредоносные предупреждения

Можно также настроить Центр управления FireSIGHT для передачи предупреждений системного журнала за событиями с определенным флагом влияния, определенным типом событий обнаружения и вредоносных событий. Чтобы сделать это, вы имеете к Части 1: Создайте Предупреждение Системного журнала и затем настройте тип событий, которые вы хотите передать к вашему серверу системного журнала. Можно сделать это путем навигации к странице **Policies> Actions> Alerts**, и затем выбора вкладки для желаемого аварийного типа.


Overview
Analysis
Policies
Devices
Objects
FireAMP
Health
System
Help
admin
Access Control
Intrusion
Files
Network Discovery
Application Detectors
Users
Correlation
Actions ▸ Alerts
Policies
Rule Editor
White List
Traffic Profiles
Alerts
Remediations
Groups
Health Monitor Alerts
Alerts
Impact Flag Alerts
Discovery Event Alerts
Advanced Malware Protection Alerts
Create Alert
Name
Type
In Use
Enabled