

# Конфигурация основного Ruleset на устройстве SSL

## Содержание

[Введение](#)

[Шаги для придержаний](#)

## Введение

Rulesets содержат правила и политику, которая управляет, как Устройство SSL обрабатывает трафик SSL. Этот документ предоставляет шаги для настройки основного ruleset на Устройстве SSL.

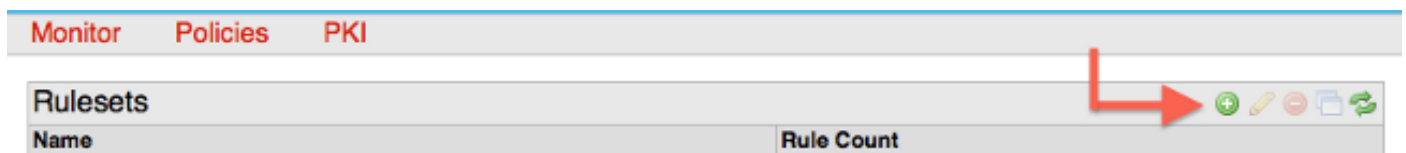
## Шаги для придержаний

Для настройки ruleset на устройстве SSL выполните действия ниже:

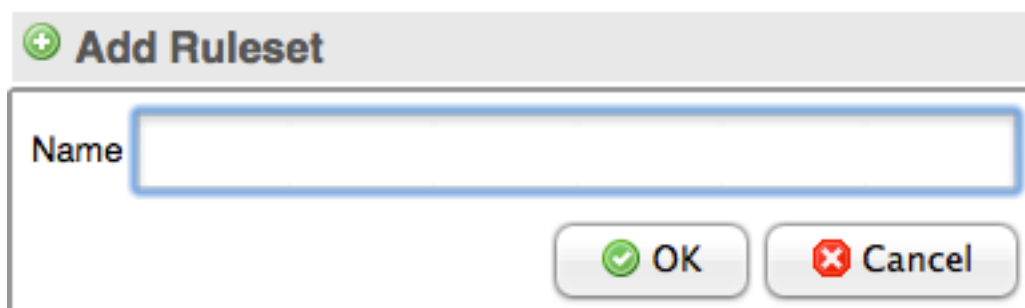
1. Перейдите **Полицейским**> **Rulesets**.



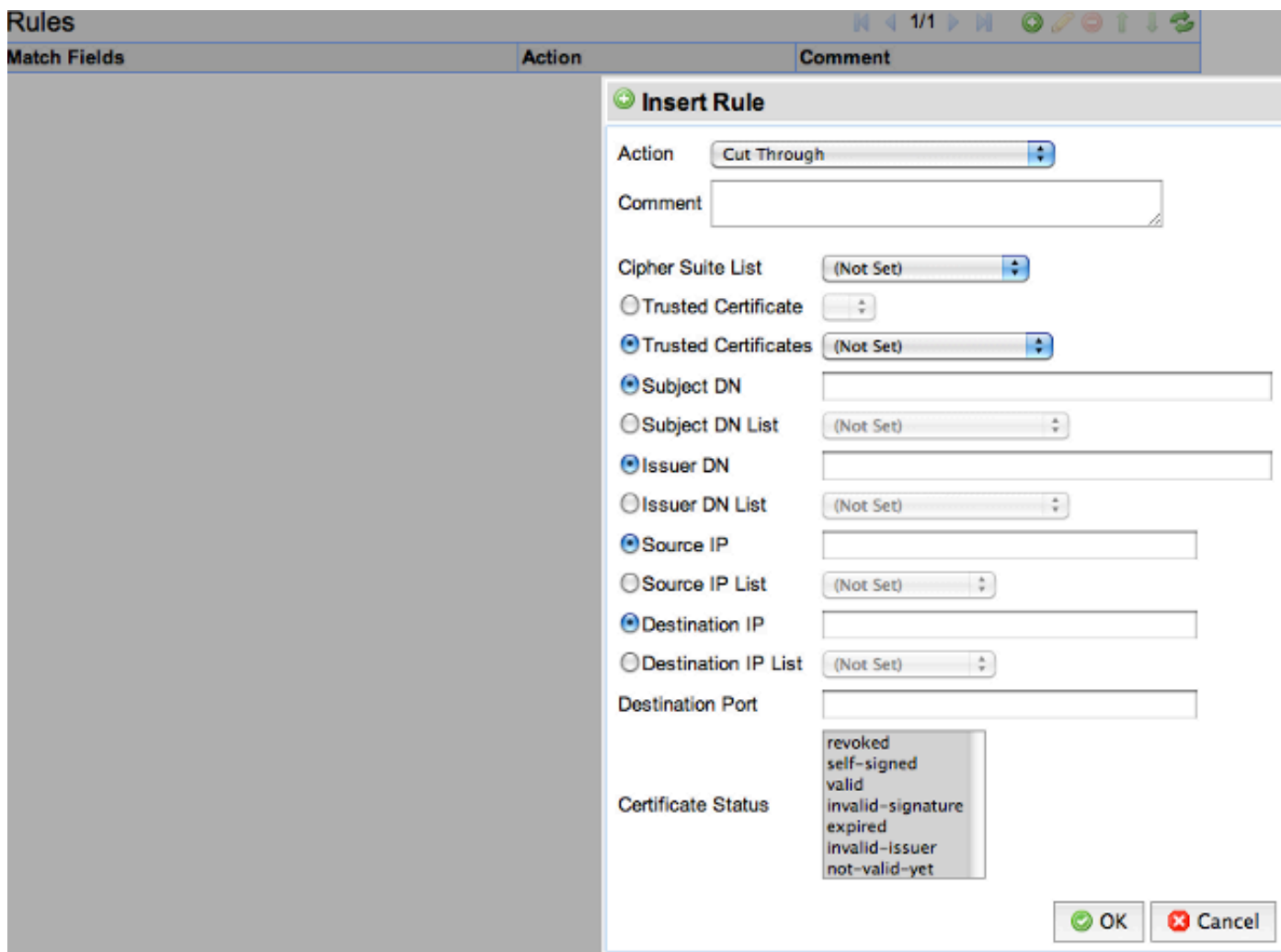
2. Выберите зеленый плюс (+), подают знак добавлять новый Ruleset.



3. Назовите Ruleset и выберите **OK**.

A screenshot of a dialog box titled 'Add Ruleset'. It features a text input field labeled 'Name' which is currently empty. Below the input field are two buttons: 'OK' with a green checkmark icon and 'Cancel' with a red X icon.

**Шаг 4.** : Из Правил раздел выбирает зеленый плюс (+) , расписываются за Правила вставить новые правила в ваш ранее созданный Ruleset. Если у вас есть множественный Rulesets, вам, вероятно, придется щелкнуть по названию Ruleset прежде, чем добавить или модифицировать правила.



Типичный Ruleset включает, но не ограниченный следующими Правилами:

1. Одно или более правил, задающих контроль с помощью известного ключа/свидетельства для трафика, переходящего к внутренним SSL - серверам, для которых можно получить ключ/свидетельство.
2. Если существуют какие-либо внутренние серверы, которые используют сертификаты клиента тогда, у вас были бы одно или более правил, что сеансы соответствия к этим серверам и прорубают трафик.
3. Если существуют внешние серверы, что вы знаете сертификаты клиента использования или что вы не хотите осматривать трафик вам , имел бы одно или более правил что трафик причины к этим серверам, которые будут прорублены.
4. Затем у вас могло бы быть действие по умолчанию, которое SAID осматривают все сеансы SSL с помощью сертификата, уходят в отставку.

**Примечание:** Всегда существует возможность, что можно осматривать трафик к узлу, который использует сертификаты клиента в пути, который означает, что сеанс является un-decryptable, и это будет означать, что откажет сеанс. Журнал сеанса покажет подробные данные сеанса и укажет, почему это было завершено, эти подробные данные предоставляют достаточные сведения для

определения прорубленного правило, которое позволит будущим сеансам успешно выполняться. Для получения дополнительной информации рассмотрите администрирование SSL и Руководство по развертыванию.