Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[Настройка](#)
[Настройка адрес назначения для выходных данных](#)
[Шаг 1. Конфигурация сервера системного журнала](#)
[Шаг 2. Конфигурация Сервера SNMP](#)
[Конфигурация для передачи Событий Трафика](#)
[Включите внешнюю регистрацию для Событий подключения](#)
[Включите внешнюю регистрацию для Событий Проникновения](#)
[Включите внешнюю регистрацию для Интеллектуальной информационной безопасности Интеллекта/DNS IP-безопасности / Интеллектуальная информационная безопасность URL](#)
[Включите внешнюю регистрацию для событий SSL](#)
[Конфигурация для передачи Системных событий](#)
[Включите внешнюю регистрацию для системных событий](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)
[Связанные обсуждения Сообщества Cisco Support](#)

Введение

Этот документ описывает модуль Огневой мощи? s система / события трафика и различный метод передачи этих событий к внешнему серверу регистрации.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание ASA (Устройство адаптивной безопасности) межсетевой экран, ASDM (Менеджер устройств адаптивной безопасности (ASDM)).
- Знание устройства огневой мощи.
- Системный журнал, знание протокола SNMP.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Модули Огневой мощи ASA (ASA 5506X/5506H-X/5506W-X, 5508-X ASA, 5516-X ASA) работающий под управлением ПО версии 5.4.1 и выше
- Модуль Огневой мощи ASA (5515-X ASA, 5525-X ASA, 5545-X ASA, 5555-X ASA) работающий под управлением ПО версии 6.0.0 и выше.
- ASDM 7.5 (1) и выше.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Тип событий

События Firepower Module могут быть категоризированы в двух типах:-

1. События трафика (События/проникновение Events/Security Intelligence Events/SSL Events/Malware/File Events соединения).
2. Системные события (события Операционной системы (OS) Огневой мощи).

Настройка

Настройка адрес назначения для выходных данных

Шаг 1. Конфигурация сервера системного журнала

Для настройки Сервера системного журнала для событий трафика Перейдите к **Конфигурации> Конфигурация Огневой мощи ASA> Политика> Предупреждения Действий** и нажмите **Создать Аварийное** раскрывающееся меню и выберите **опцию Create Syslog Alert.** Введите значения для Сервера системного журнала.

Name: Задайте название, которое однозначно определяет Сервер системного журнала.

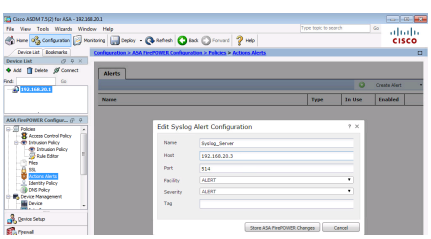
Хост:Задайте IP-адрес / имя хоста Сервера системного журнала.

Порт: Задайте номер порта Сервера системного журнала.

Средство: Выберите любое средство

Степени серьезности ошибки: Выберите любые Степени серьезности ошибки, которые настроены на вашем Сервере системного журнала.

Метка: Задайте имя тега, что вы хотите появиться с Сообщением системного журнала.



Шаг 2. Конфигурация Сервера SNMP

Для настройки сервера TRAP-СООБЩЕНИЯ SNMP для событий трафика **Конфигурации ASDM> Конфигурация Огневой мощи ASA> Политика> Предупреждения Действий** и нажмите **Создать Аварийное** раскрывающееся меню и выберите **опцию Create SNMP Alert.**

Name:Задайте название, которое однозначно определяет сервер TRAP-СООБЩЕНИЯ SNMP.

Сервер trap-сообщения:

Version :

Строка имени и пароля: при выборе **Version** Задайте название сообщества SNMP.

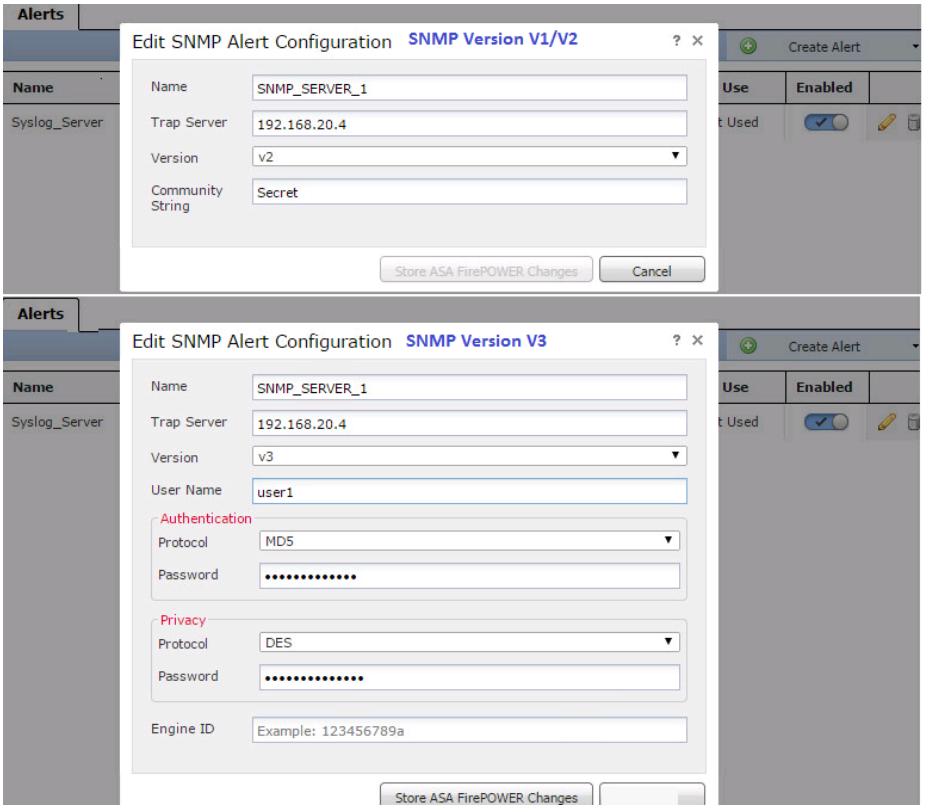
Имя пользователя: Version, поле **User Name** системных приглашений. Задайте имя пользователя.

Аутентификация: Эта опция является частью конфигурации v3 SNMP. Это предоставляет аутентификацию на основе Хэша

алгоритм с помощью или MD5 или алгоритмов SHA. В **Протоколе** выпадающее меню выбирает алгоритм хэширования и входит

пароль в **Параметре пароля** . Если вы не хотите использовать эту функцию, то выберите опцию **None**.

Конфиденциальность: Эта опция является частью конфигурации v3 SNMP. Это предоставляет шифрование с помощью алгоритма DES. В **Протоколе** меню отбрасывания выбирает опцию, поскольку **DES&** вводят пароль в **Поле Password**. Если вы не хотите использовать функцию шифрования данных, затем выбирать опцию **None**.



Конфигурация для передачи Событий Трафика

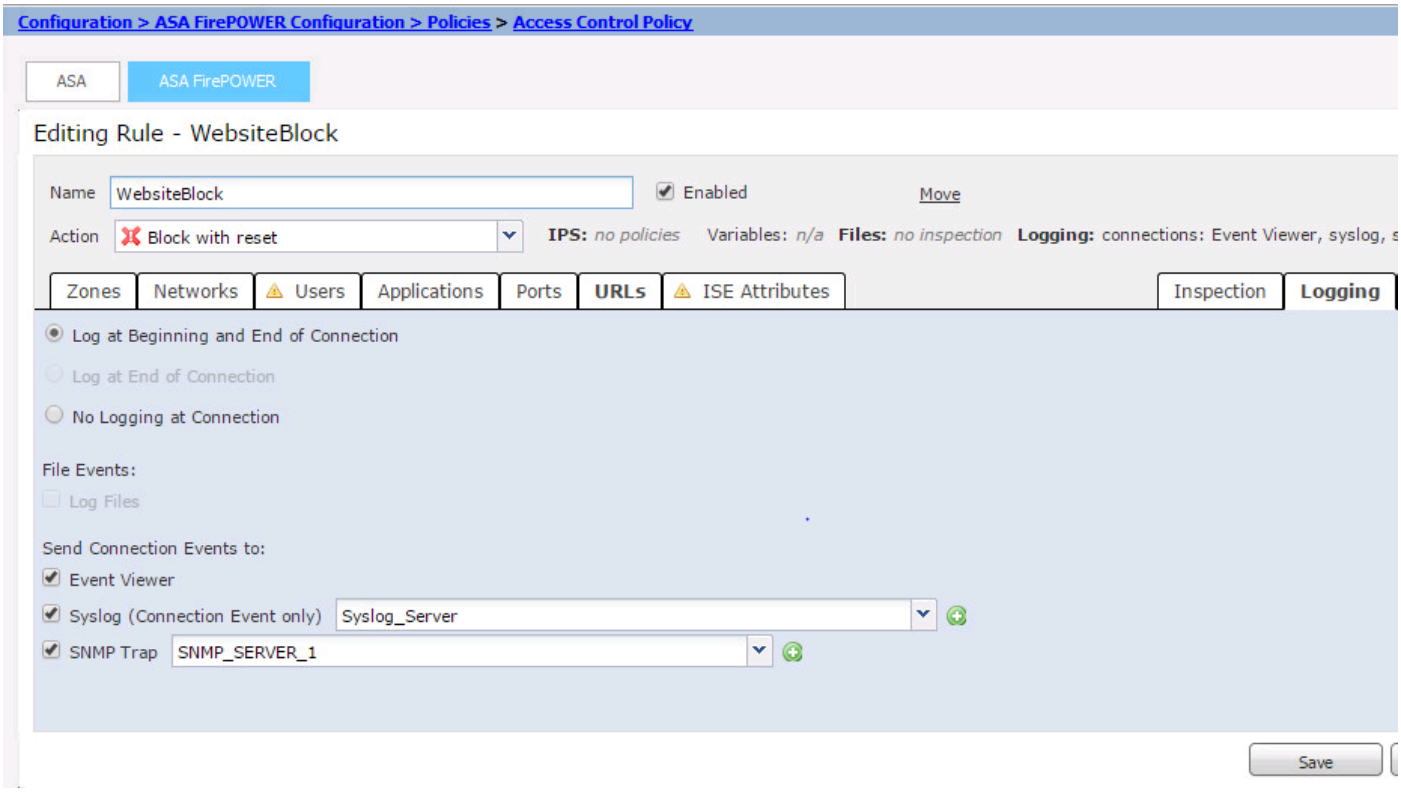
Включите внешнюю регистрацию для Событий подключения

Когда трафик поражает правило доступа logging enabled, события подключения генерируются. Для включения внешней регистрации для событий подключения перейдите к **(Конфигурация ASDM> Конфигурация Огневой мощи ASA>** редактируют **правило доступа** и перешли к **параметру регистрации**.

Выберите параметр регистрации или **журнал вначале и Конец Соединения** или **журнал в конце Соединения**. Перейдите, чтобы **Передать События подключения к** опции и задать, куда передать события.

Для передачи событий к внешнему серверу системного журнала выберите **Syslog**, и затем выберите ответ предупреждения Syslog от выпадающего списка. Дополнительно, можно добавить ответ предупреждения Системного журнала путем нажатия добавить **значка**.

Для передачи событий подключения к серверу trap-сообщения SNMP выберите **SNMP Trap**, и затем выберите ответ предупреждения SNMP от выпадающего списка. Дополнительно, можно добавить ответ предупреждения SNMP путем нажатия добавить **значка**.



Включите внешнюю регистрацию для Событий Проникновения

Когда подпись (правила фырканья) совпадает с некоторым вредоносным трафиком, события проникновения генерируются. включения внешней регистрации для событий проникновения перейдите к **Конфигурации ASDM> Конфигурация Огневой мощи ASA>** Или создайте новую политику Проникновения или отредактируйте существующую Политику Проникновения. Перейдите к **Расширенной настройке> Внешние Ответы.**

Для передачи событий проникновения к внешнему серверу SNMP выберите опцию **Enabled**

в **Предупреждении SNMP** и затем нажмите **опцию Edit**.

Тип ловушки: тип ловушки используется для IP-адресов, которые появляются в предупреждениях. Если ваша система управления сетью правильно представляет тип адреса INET_IPV4, то можно выбрать как Двоичные файлы. В противном случае выберите как Строка.

Версия SNMP: Выберите кнопка с зависимой фиксацией **Version 3** или **Version 2**.

Опция SNMP v2

Сервер trap-сообщения: Задайте IP-адрес / имя хоста сервера TRAP-СООБЩЕНИЯ SNMP, как показано в этом образе.

Строка имени и пароля: Задайте название сообщества.

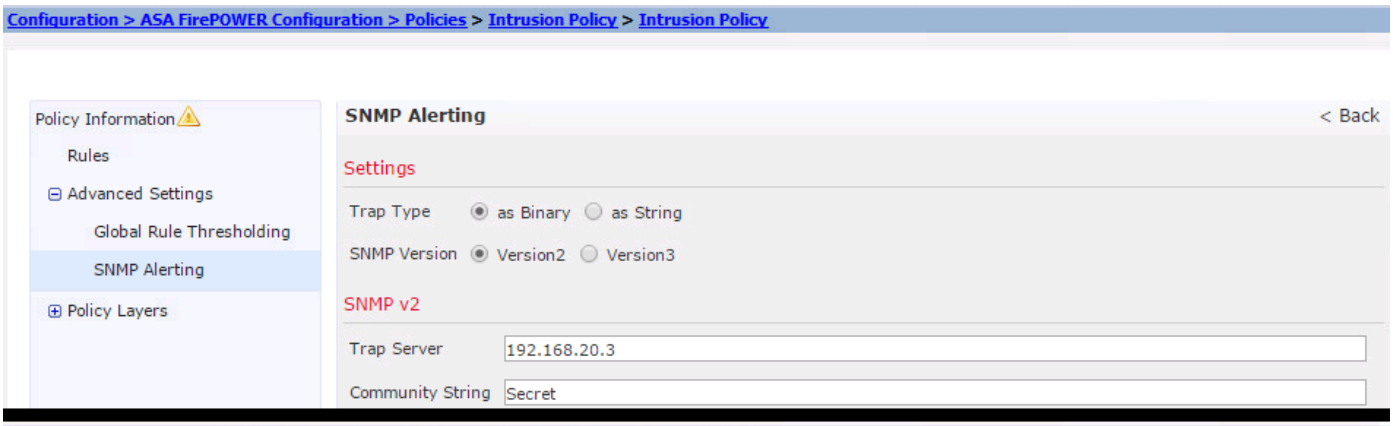
Опция v3 SNMP

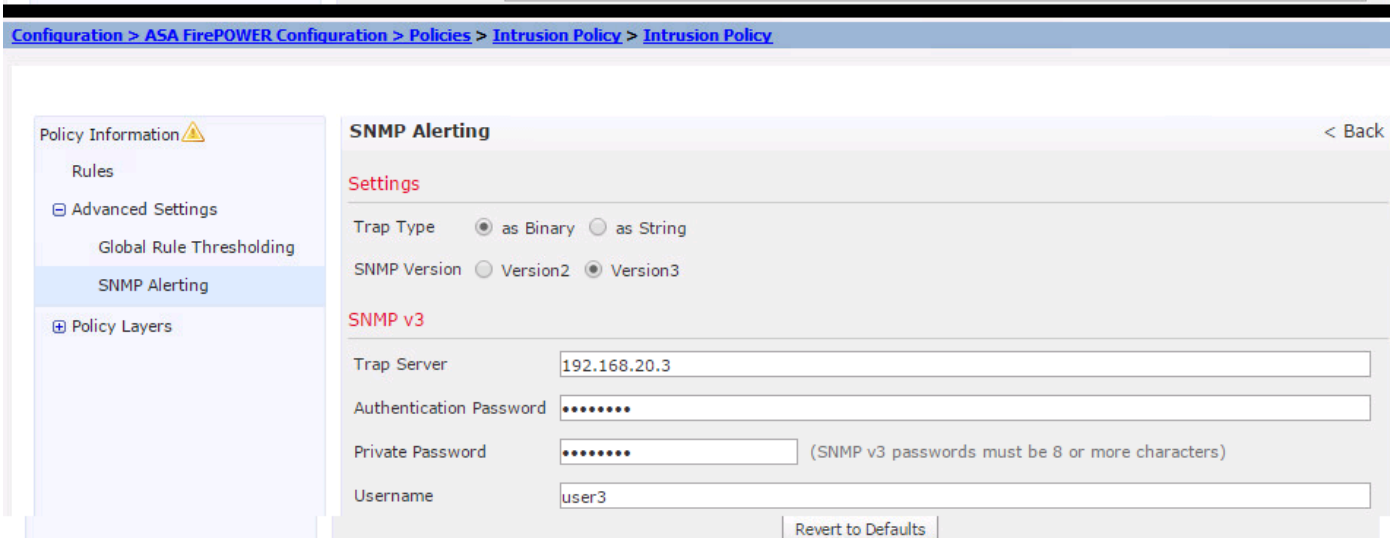
Сервер trap-сообщения: Задайте IP-адрес / имя хоста сервера TRAP-СООБЩЕНИЯ SNMP, как показано в этом образе.

Пароль для проверки подлинности: Specifypassword требуется для аутентификации. V3 SNMP использует хэш-функцию для аутентификации

Частный Пароль: Задайте пароль для шифрования. V3 SNMP использует блочный шифр Стандарта шифрования данных (DES) для шифрования этого пароля.

Имя пользователя: Задайте имя пользователя.





Для передачи событий проникновения к внешнему серверу системного журнала выберите опцию Enabled in Syslog Alerting , тогда нажимают **опцию Edit**, как показано в этом образе.

Logging host #.#.#.#: Задайте IP-адрес / имя хоста Сервера системного журнала.

Средство: Выберите любое средство , которое настроено на вашем Сервере системного журнала.

Степени серьезности ошибки: Выберите любые Степени серьезности ошибки, которые настроены на вашем Сервере системного журнала.

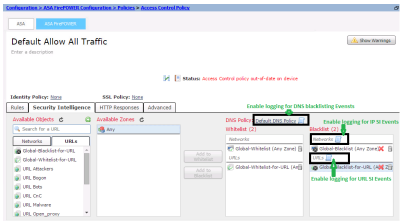
Включите внешнюю регистрацию для Интеллектуальной информационной безопасности Интеллекта/DNS IP-безопасности / Интеллектуальная информационная безопасность URL

Когда трафик совпадает с любым IP-адресом / доменное название/URL база данных Интеллектуальной информационной безопасности, **интеллектуальная информационная безопасность Интеллекта/DNS IP-безопасности /** события **Security Intelligence URL** генерируется. Для включения внешней регистрации для IP / События Интеллектуальной информационной безопасности URL/DNS, перейдите к **(Конфигурация ASDM> Конфигурация Огневой мощи ASA>**,

Нажмите **значок** как показано в образе для включения регистрации для Интеллектуальной информационной безопасности IP/DNS/URL. Нажатие значка побуждает диалоговое окно к enable logging и опции передавать события к внешнему серверу.

Для передачи событий к внешнему серверу системного журнала выберите **Syslog**, и затем выберите ответ предупреждения Syslog от выпадающего списка. Дополнительно, можно добавить ответ предупреждения Системного журнала путем нажатия добавить значка.

Для передачи событий подключения к серверу trap-сообщения SNMP выберите **SNMP Trap**, и затем выберите ответ предупреждения SNMP от выпадающего списка. Дополнительно, можно добавить ответ предупреждения SNMP путем нажатия добавить значка.



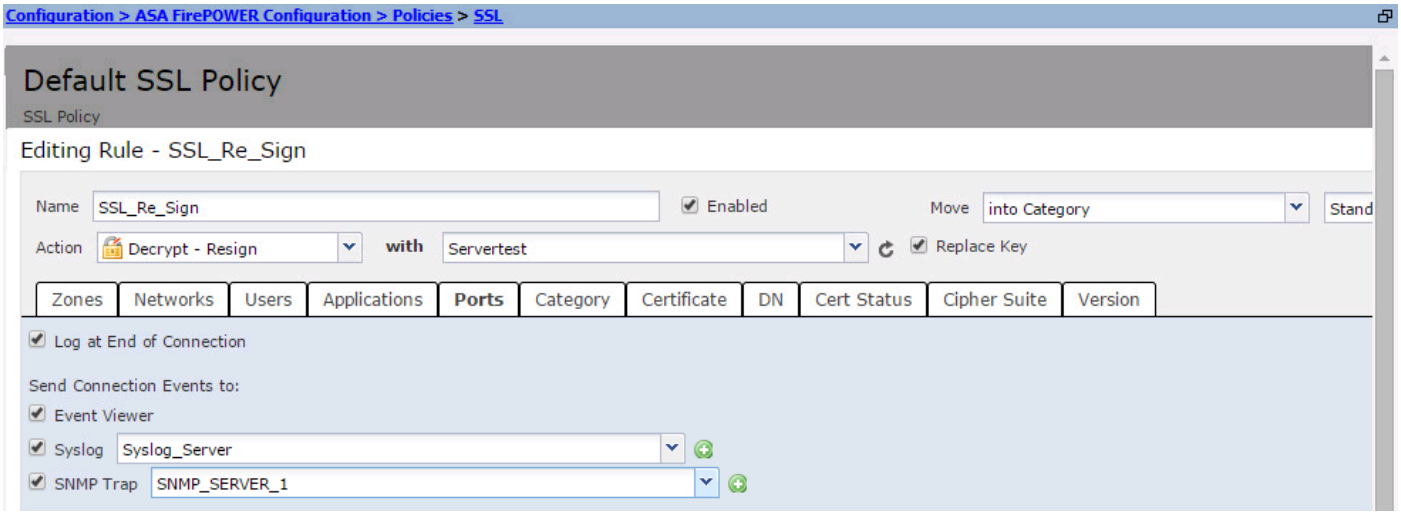
Включите внешнюю регистрацию для событий SSL

События SSL генерируются, когда трафик совпадает с любым правилом в политике SSL, в которой включена регистрация. Для включения внешней регистрации для трафика SSL перейдите к **Конфигурации ASDM> Конфигурация Огневой мощи ASA>**Отредактируйте существующее или создайте новое правило и перейдите к **параметру регистрации**. Выберите **журнал в конце Параметра подключения**.

Затем перейдите, чтобы **Передать События подключения к** и задать, куда передать события.

Для передачи событий к внешнему серверу системного журнала выберите **Syslog**, и затем выберите ответ предупреждения Syslog от выпадающего списка. Дополнительно, можно добавить ответ предупреждения Системного журнала путем нажатия добавить значка.

Для передачи событий подключения к серверу trap-сообщения SNMP выберите **SNMP Trap**, и затем выберите ответ предупреждения SNMP от выпадающего списка. Дополнительно, можно добавить ответ предупреждения SNMP путем нажатия добавить значка.



Конфигурация для передачи Системных событий

Включите внешнюю регистрацию для системных событий

Системные события показывают статус Операционной системы Огневой мощи. Диспетчер SNMP может использоваться для опроса этих системных событий.

Для настройки сервера SNMP для опроса системных событий от Модуля Огневой мощи необходимо настроить Системную политику, которая делает доступную информацию в MIB огневой мощи (Информационная база управления), которая может быть опрошена сервером SNMP.

Перейдите к **Конфигурации ASDM> Конфигурация Огневой мощи ASA>** и нажмите **SNMP**.

Версия SNMP: поддержки модулей SNMP v1/v2/v3 Огневой мощи. Задайте версию SNMP.

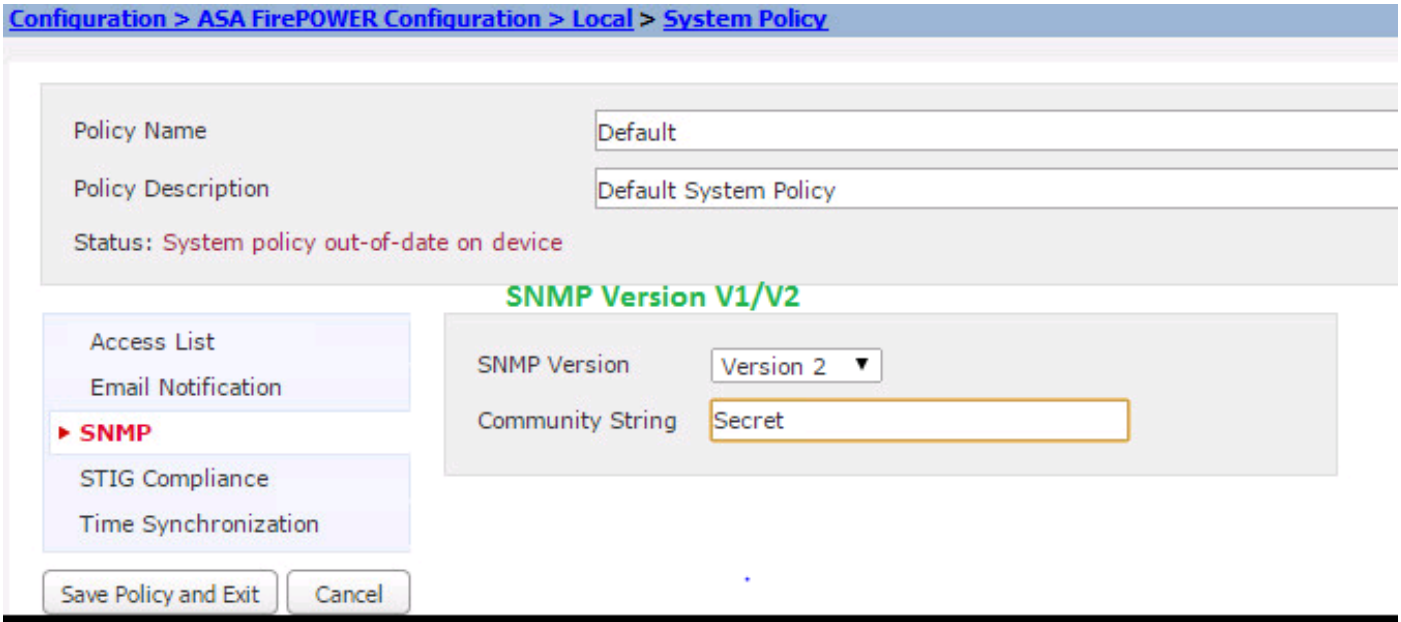
Строка имени и пароля: Если вы выбираете **v1 / v2** в опции версии SNMP, вводите имя сообщества SNMP в поле Community String.

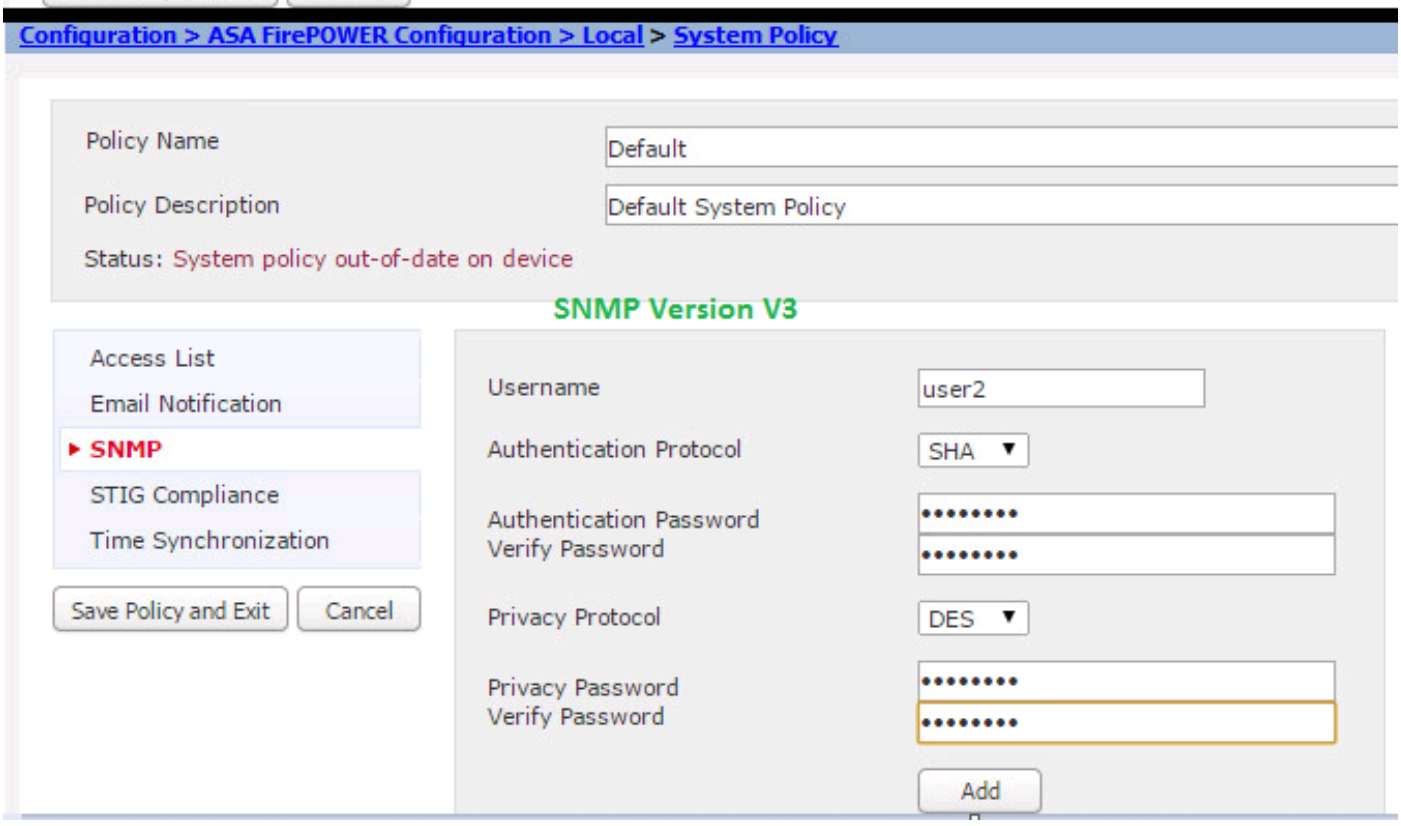
Имя пользователя: Если вы выбираете опцию **v3** в опции версии. Нажмите **Добавить кнопку User Имя пользователя** в поле имени пользователя.

Аутентификация: Эта опция является частью конфигурации v3 SNMP. Это предоставляет аутентификацию на основе Хешированного Кода аутентификации сообщения **Protocol** для алгоритма хэширования и введите пароль

в **Поле Password**. Если вы не хотите использовать характеристику проверки подлинности, тогда выбирают опцию **None**.

Конфиденциальность: Эта опция является частью конфигурации v3 SNMP. Это предоставляет шифрование с помощью алгоритма DES/AES. Выберите протокол **Поле Password**. Если вы не хотите функцию шифрования данных, тогда выбирают опцию **None**.





Примечание: Информационная база управления (MIB) является набором сведений, который организован

иерархически. Файл Mib (DCEALERT.MIB) для Модуля Огневой мощи доступен в расположении каталогов (/etc/sf/DCEALERT.MIB), который может быть выбран от этого расположения каталогов.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация