Содержание

Введение

Этот документ описывает Сетевую Усовершенствованную вредоносную защиту (AMP) / функциональность контроля за доступом к файлу модуля FirePOWER и метода для настройки их с Менеджером устройств адаптивной безопасности (ASDM) (ASDM).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание межсетевого экрана Устройства адаптивной защиты (ASA) и ASDM.
- Знание устройства FirePOWER.

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 позже.
- Модуль Огневой мощи ASA (5515-X ASA, 5525-X ASA, 5545-X ASA, 5555-X ASA), которые работают под управлением ПО версии 6.0.0 и позже.
- ASDM 7.5.1 и позже.

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

Вредоносное программное обеспечение / вредоносное ПО может войти в сети организации через несколька способов. Чтобы определить и смягчить эффекты этого вредоносного программного обеспечения и вредоносного ПО, функции AMP FirePOWER's могут быть использованы, чтобы обнаружить и дополнительно заблокировать передачу вредоносного программного обеспечения и вредоносного ПО в сети.

С функциональностью управления файлом можно принять решение контролировать (обнаруживают), блокируют или позволяют передачу выгрузки файла и загрузку. Например, политика файла может проводиться, который блокирует загрузку исполняемых файлов пользователем.

С Сетевой функциональностью AMP можно выбрать типы файла, что вы хотите контролировать обычно используемые протоколы и передать хэши SHA 256, метаданные от файлов, или даже копии самих файлов к Интеллектуальному Облаку Cisco Security для вредоносного анализа. Облако возвращает расположение для хэшей файла как чистое или злонамеренное на основе анализа файла.

Управление файлом и AMP для Огневой мощи могут настраиваться как политика файла и использоваться в качестве части вашей полной конфигурации управления доступом. Политика файла, привязанная к правилам управления доступом, осматривает сетевой трафик, который удовлетворяет условиям правила.

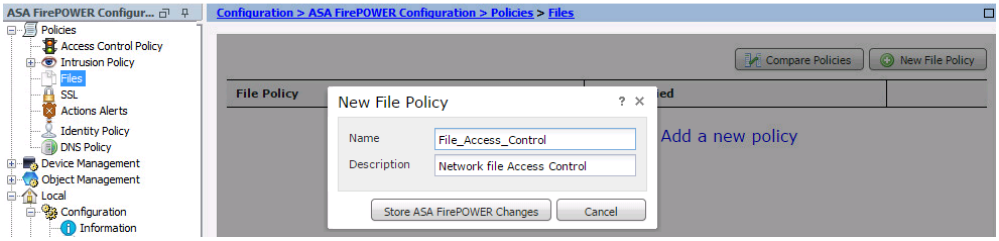
> **Примечание:** Гарантируйте, что Модуль FirePOWER имеет Защищать/Управлять/Вредоносное ПО лицензию для настройки этой функциональности. Для проверки лицензий выберите **Configuration> ASA FirePOWER Configuration> License.**

Настройте политику файла для управления файлом / сетевой AMP

Управление доступом файла конфигурации

Войдите к ASDM и выберите **Configuration> ASA Firepower Configuration> Policies> Files.** появляется.

Введите Имя и дополнительное описание для вашей новой политики, затем нажмите опцию **Store ASA Firepower Changes**. Страница File Policy Rule появляется.



Нажмите Add Правило Файла для добавления правила к политике файла. Правило файла дает вам гранулированный контроль над типами файла, которые вы хотите регистрировать, заблокировать, или просмотр для вредоносного ПО.

Протокол уровня приложения: Задайте прикладной протокол или как **Любой** (по умолчанию) или как определенный протокол (HTTP, SMTP, IMAP, POP3, FTP, SMB).

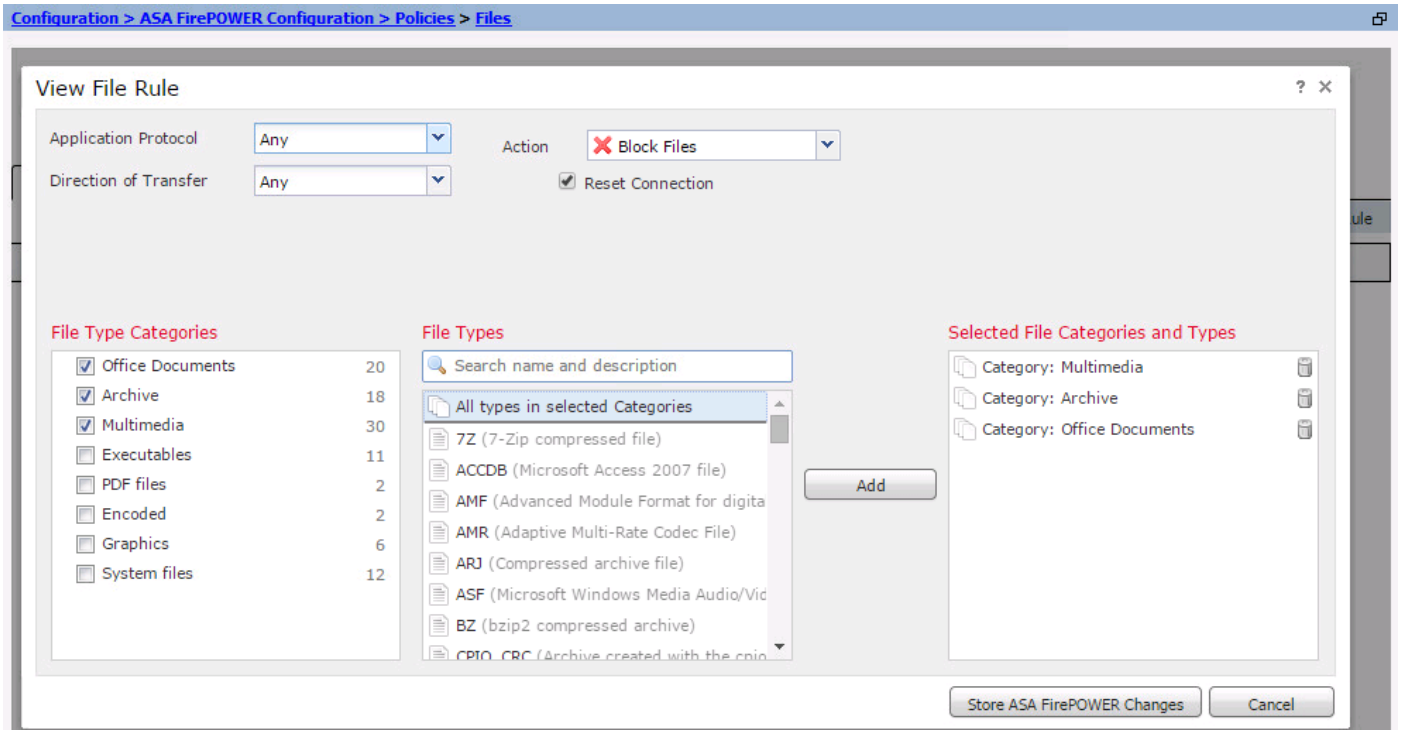
Направление Передачи: Задайте направление передачи файла. Это мог быть или Любой или Загрузка/Загрузка на основе Прикладного протокола. Можно осмотреть протокол (HTTP, IMAP, POP3, FTP, SMB) для загрузки файла и протокола (HTTP, SMTP, FTP, SMB) для выгрузки файла. Используйте **Любую** опцию для обнаружения файлов по протоколам составного приложения, независимо от того, передают ли пользователи или получают файл.

Действие: Задайте Действие для функциональности Контроля за Доступом к файлу. Действие было бы или **Обнаружить Файлы** или **Блочные Файлы.** действие **Файла**, генерирует событие, и **Блочное** действие **Файлов** генерируют событие и блокируют передачу файла. С **Блочным** действием **Файлов** можно дополнительно выбрать **Reset Connection** для завершения соединения.

Категории Типа файла: Выберите File Type Categories, для которого вы хотите или заблокировать файл или генерировать предупреждение.

Типы файла: Выберите Типы файла. Опция File Types дает более гранулированную опцию для выбора определенного типа файла.

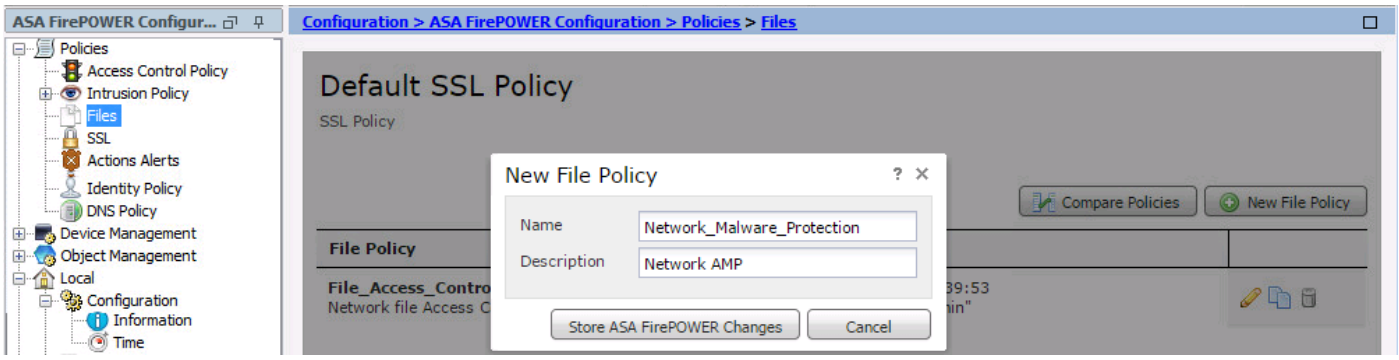
Выберите опцию **Store ASA Firepower Changes** для сохранения конфигурации.



Настройте сетевую вредоносную защиту (сетевой AMP)

Войдите к ASDM и перейдите к **Конфигурации> Конфигурация Огневой мощи ASA> Политика> Файлы.** Страница Policy Файла появляется. Теперь щелкните , Новое диалоговое окно Policy Файла появляется.

Введите **Имя** и **дополнительное описание** для вашей новой политики, затем щелкните по опции **Store ASA Firepower Changes**. Страница File Policy Rules появляется.



Нажмите опцию **Add File Rule** для добавления правила подать политику. Правило файла дает вам гранулированный контроль над типами файла, которые вы хотите регистрировать, заблокировать, или просмотр для вредоносного ПО.

Протокол уровня приложения: Задайте или Любой или определенный протокол (по умолчанию) (HTTP, SMTP, IMAP, POP3, FTP, SMB)

Направление Передачи: Задайте направление передачи файла. Это мог быть или Любой или Загрузка / Загрузка на основе Прикладного протокола. Можно осмотреть протокол (HTTP, IMAP, POP3, FTP, SMB) для загрузки файла и протокола (HTTP, SMTP, FTP, SMB) для выгрузки файла. Используйте **Любую** опцию для обнаружения файлов по протоколам составного приложения, независимо от пользователей, передающих или получающих файл.

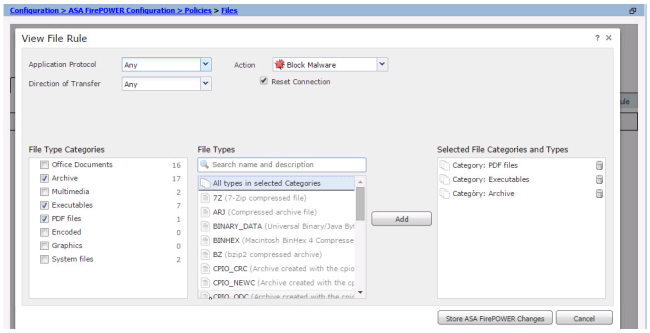
Действие: Для Сетевой Вредоносной функциональности Защиты Действие было бы или **Вредоносным Облачным Поиском** или **Блочным Вредоносным ПО. Облачный Поиск Вредоносного ПО** действия генерирует только событие, тогда как **Вредоносное ПО Блока** действия генерирует событие, а также заблокируйте вредоносную передачу файла.

> **Примечание: Вредоносный Облачный Поиск andBlock Вредоносные** правила позволяет, что Огневая мощь для вычисления SHA 256 хеширует и передает его за облачным процессом поиска, чтобы определить, содержат ли файлы, пересекающие сеть, вредоносное ПО.

Категории Типа файла: Выберите определенные Категории Файла.

Типы файла: Выберите определенные **Типы файла** для большего количества гранулированных типов файла.

Выберите **опцию Store ASA Firepower Changes** для сохранения конфигурации.



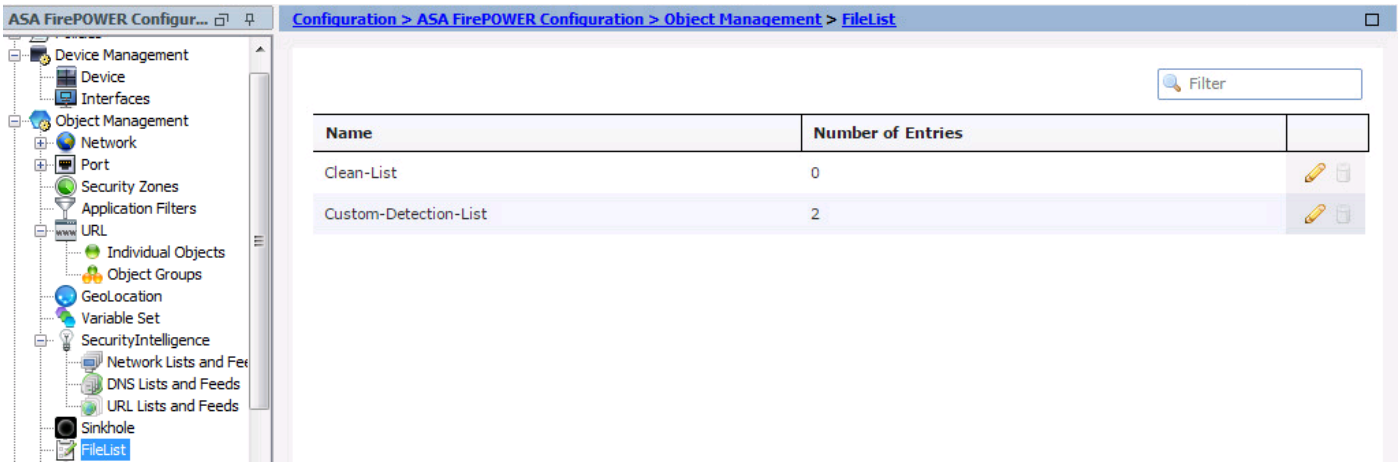
Примечание: Политика файла обрабатывает файлы в следующем заказе действия

правила: Блокирование имеет приоритет по вредоносному контролю, который имеет приоритет по простому обнаружению и регистрации.

Если вы настраиваете сетевую усовершенствованную вредоносную защиту (AMP), и Облако Cisco неправильно обнаруживает файл? s расположение, можно добавить, что файл к списку файлов с помощью значения хеш-функции SHA 256 для улучшения обнаруживает расположение файла в будущем. в зависимости от типа списка файлов можно сделать:

- Для обработки файла, как будто облако назначило чистое расположение добавьте файл к чистому списку.
- Для обработки файла, как будто облако назначило вредоносное расположение добавьте файл к пользовательскому списку.

Для настройки этого перейдите к **Конфигурации> конфигурация ASA FirePOWER> Управление объектами> Список файлов** и отредактируйте список для добавления SHA 256.



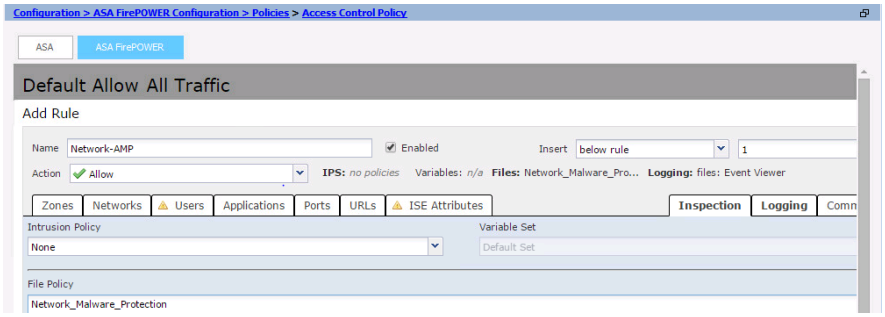
Настройте политику контроля доступа для политики файла

Перейдите к **Конфигурации> Конфигурация Огневой мощи ASA>** и создайте или новый **Доступ, управляют** или редактируют существующее **Правило Доступа,** как показано в этом образе.

К Политике файла конфигурации Действие должно быть**, Позволяют**. Перейдите к вкладке **Inspection** и выберите **File Policy** из выпадающего меню.

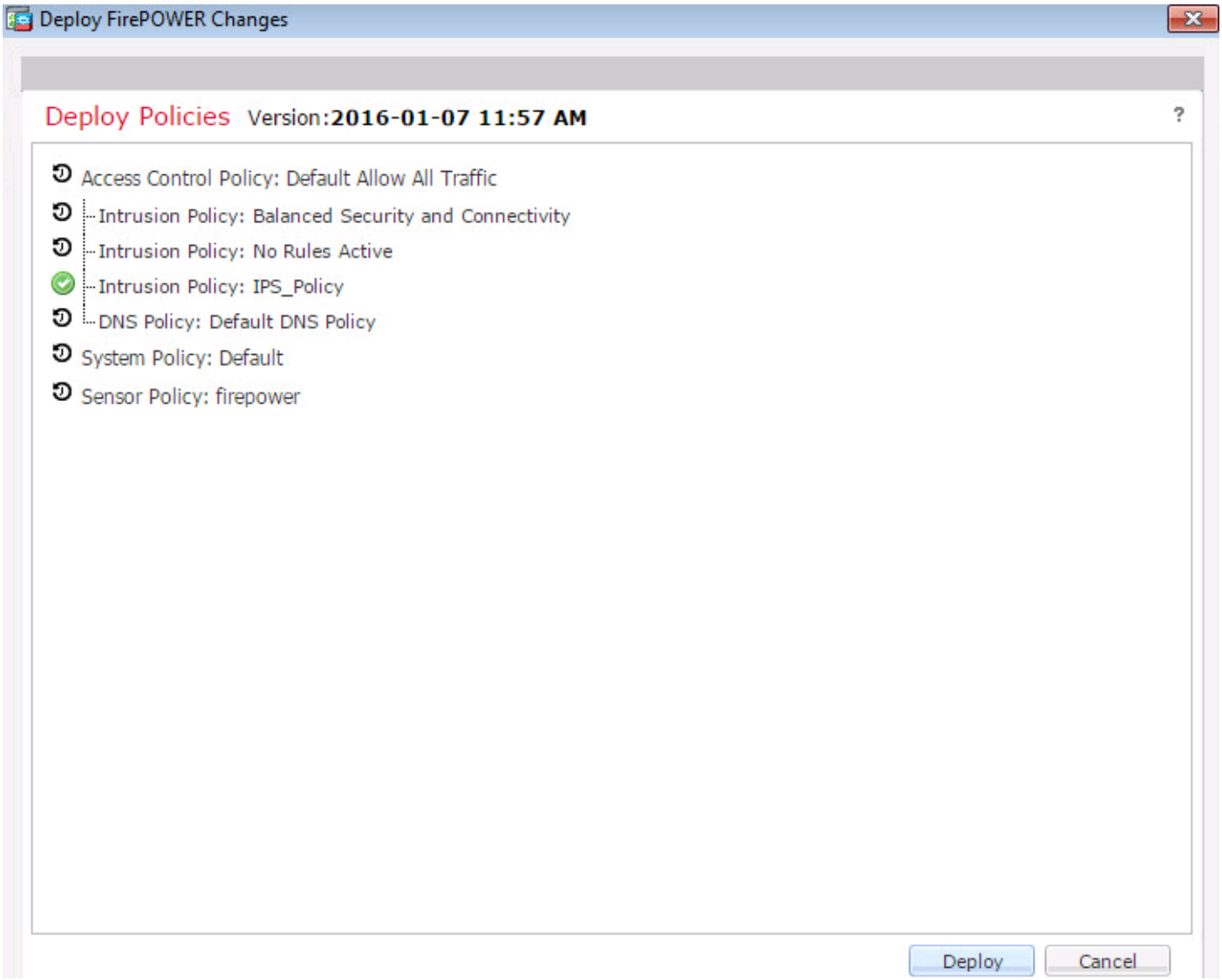
К enable logging переместитесь **по параметру регистрации** и выберите соответствующий параметр регистрации и опцию **Log Files**. Нажмите **кнопку Save/Add** для сохранения конфигурации.

Выберите **опцию Store ASA Firepower Changes** для сохранения изменений политики AC.



Разверните политику контроля доступа

Перейдите к опции **Deploy** ASDM и выберите опцию **Deploy Firepower Change** из выпадающего меню. Щелкните по опции **Deploy** для развертывания изменений.

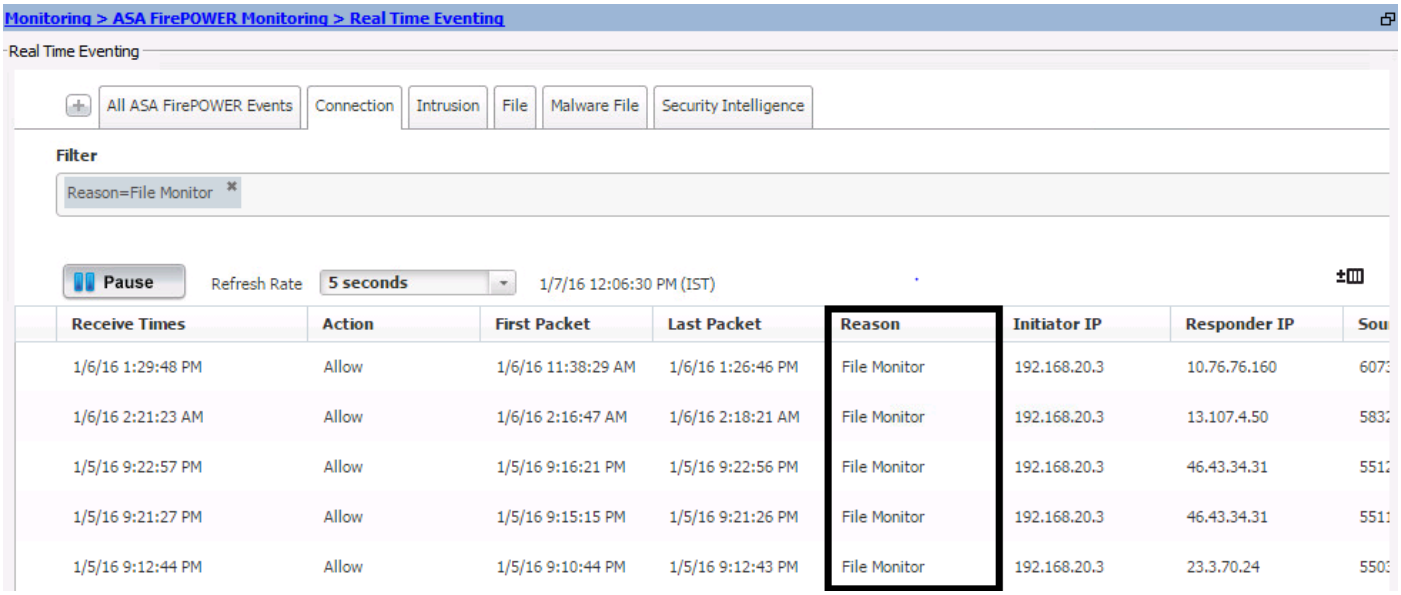


Перейдите к **Мониторингу> Мониторинг Огневой мощи ASA> Статус Задачи.** Гарантируйте, что задача должна завершить для применения изменения конфигурации.

> **Примечание:** В версии 5.4.x, Для применения Политики доступа к датчику вам нужно к **Изменениям clickApply ASA FirePOWER.**

Соединение монитора для событий Policy файла

Чтобы видеть, что события, генерируемые Модулем Огневой мощи, отнесенным к политике файла, перешли к **Мониторингу> Мониторинг Огневой мощи ASA> Оперативная Обработка событий.**



Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Гарантируйте, что Политика Файла правильно conifigured с протоколом / направление / Действие / Типы файла. Гарантируйте, что корректная Политика Файла включала в Правила Доступа.

Гарантируйте, что развертывания Политики контроля доступа завершают успешно.

Контролируйте События подключения и События файла (**Контролирующий> Мониторинг Огневой мощи ASA> Оперативная Обработка событий**), чтобы проверить, поражает ли трафик корректное правило или нет.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация