قم بتكوين الوحدة النمطية FirePOWER للشبكة AMP أو التحكم في الملفات باستخدام ASDM.

المحتويات

المقدمة

يصف هذا المستند وظيفة التحكم في الوصول إلى الملفات/الحماية المتقدمة من البرامج الضارة للشبكة (AMP) للوحدة النمطية FirePOWER وطريقة تكوينها باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة جدار حماية أجهزة الأمان المعدلة (ASA) و ASDM.
- معرفة جهاز أمان FirePOWER.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الوحدات النمطية ASA FirePOWER (ASA 5506X/5506H-X/5506W-X، ASA 5508-X، ASA 5516-X) التي تشغل الإصدار 5.4.1 والإصدارات الأحدث.
- الوحدة النمطية ASA FirePOWER (ASA 5515-X، ASA 5525-X، ASA 5545-X، ASA 5555-X)

التي تشغل الإصدار 6.0.0 من البرنامج والإصدارات الأحدث.
- ASDM 7. 5. 1 والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يمكن أن تدخل البرامج/البرامج الضارة الضارة في شبكة مؤسسة من خلال طرق متعددة. تحديد تأثيرات هذا البرنامج والبرنامج الضار وتخفيفها، يمكن إستخدام ميزات AMP الخاصة ب FirePOWER الكتشاف نقل البرامج والبرامج الضارة في الشبكة وحظره إختياريا.

باستخدام وظيفة التحكم في الملفات، يمكنك إختيار مراقبة (الكشف) تحميل الملفات وتنزيلها أو حظرها أو السماح بنقل هذه الملفات. على سبيل المثال، يمكن تنفيذ نهج الملف الذي يمنع تنزيل الملفات القابلة للتنفيذ بواسطة المستخدم.

باستخدام وظيفة AMP للشبكة، يمكنك تحديد أنواع الملفات التي ترغب في مراقبتها عبر البروتوكولات المستخدمة بشكل شائع وإرسال تجزئة SHA 256 أو بيانات التعريف من الملفات وأ حتى نسخ من الملفات نفسها إلى مجموعة Cisco Security Intelligence لتحليل البرامج الضارة. ترجع السحابة المصير النهائي لتجزئة الملفات على أنه نظيف أو ضار وأ استنادا إلى تحليل الملف.

يمكن تكوين التحكم في الملفات و AMP ل FirePOWER كنهج ملف واستخدامها كجزء من التكوين العام للتحكم في الوصول. تقوم سياسات الملفات المرتبطة بقواعد التحكم في الوصول بفحص حركة مرور الشبكة التي تفي بشروط القواعد.

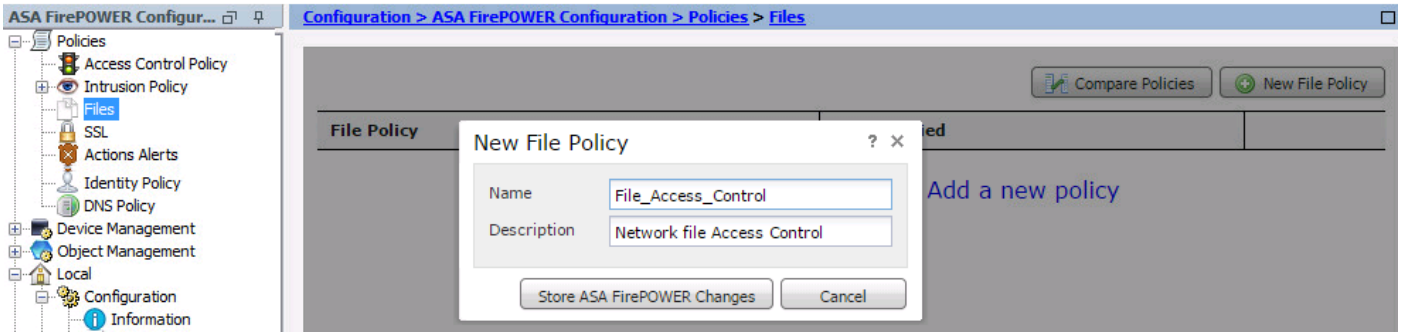
> **ملاحظة**: تأكد من أن وحدة FirePOWER تحتوي على ترخيص حماية/تحكم/برنامج ضار لتكوين هذه الوظيفة. للتحقق من الترخيص، أختر **التكوين > تكوين ASA FirePOWER > الترخيص**.

تكوين نهج الملف ل File Control/Network AMP

تكوين التحكم في الوصول إلى الملف

سجل الدخول إلى ASDM واختر **التكوين > ASA Firepower Configuration > السياسات > الملفات**. يظهر مربع الحوار **نهج ملف جديد**.

أدخل اسما ووصفا إختياريا للنهج الجديد، ثم انقر فوق خيار **تخزين تغييرات ASA FirePOWER**. تظهر صفحة قاعدة نهج الملف.



انقر فوق **إضافة قاعدة ملف** لإضافة قاعدة إلى نهج الملف. تمنحك قاعدة الملف التحكم متعدد المستويات في أنواع الملفات التي تريد تسجيلها أو حظرها أو مسحها ضوئيا بحثا عن برامج ضارة.

بروتوكول التطبيق: حدد بروتوكول التطبيق على أنه إما **أي** (افتراضي) أو البروتوكول المحدد (HTTP و SMTP و IMAP و POP3 و FTP و SMB).

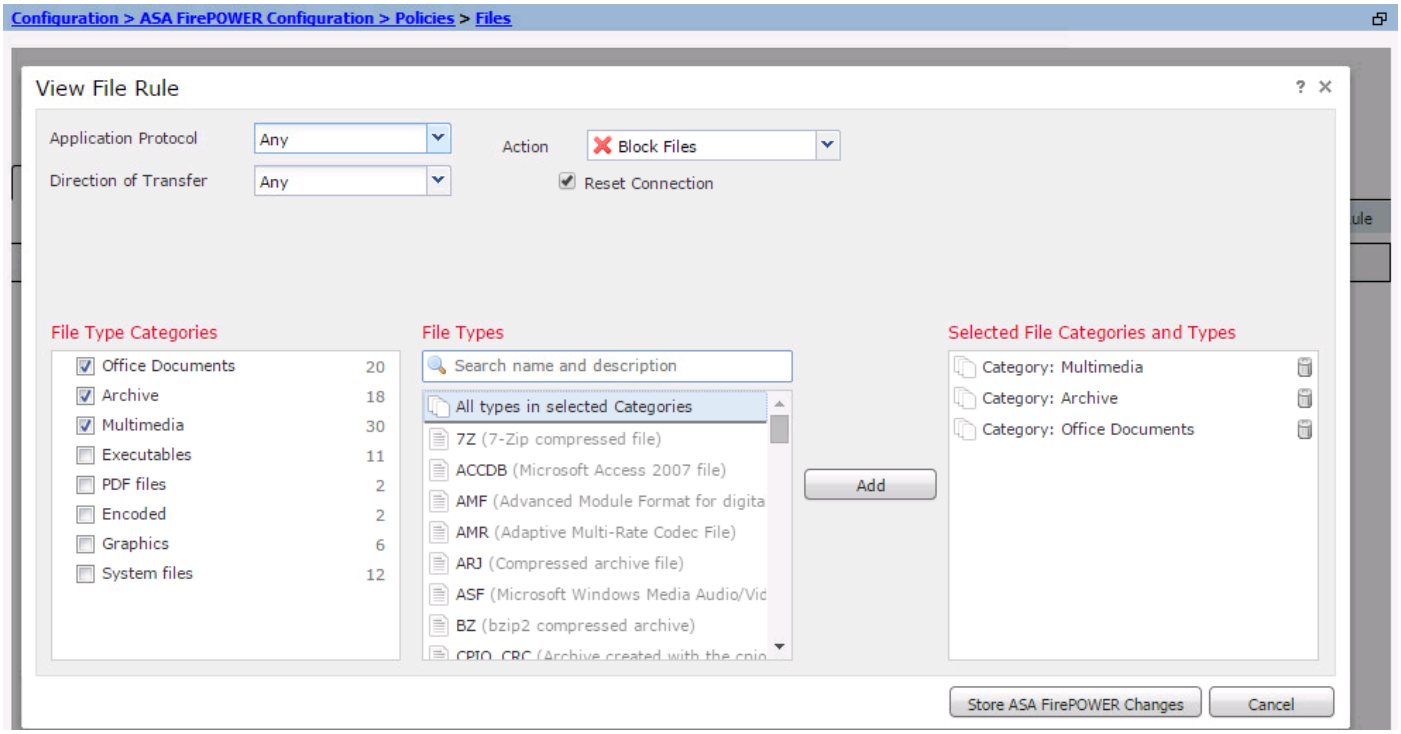
اتجاه النقل: حدد إتجاه نقل الملف. يمكن أن يكون أي أو تحميل/تنزيل استنادا إلى بروتوكول التطبيق. يمكنك فحص البروتوكول (HTTP و IMAP و POP3 و FTP و SMB) لتنزيل الملف والبروتوكول (HTTP و SMTP و FTP و SMB) لتحميل الملف. أستخدم الخيار **أي** لاكتشاف الملفات عبر بروتوكولات تطبيق متعددة، بغض النظر عما إذا كان المستخدمون يرسلون الملف أو يتلقونه.

الإجراء: تحديد الإجراء لوظيفة التحكم في الوصول إلى الملف. سيكون الإجراء إما **كشف الملفات** أو **حظر الملفات. كشف** عملية **ملف** يولد الحدث **وحظر** إجراء **ملفات** يولد الحدث ويمنع إرسال الملف. باستخدام الإجراء **حظر الملفات** ، يمكنك إختياريا تحديد **إعادة ضبط الاتصال** لإنهاء الاتصال.

فئات نوع الملف: حدد فئات نوع الملف التي تريد حظر الملف لها أو إنشاء التنبيه.

أنواع الملفات: حدد أنواع الملفات. يعطي خيار أنواع الملفات خيار أكثر دقة لاختيار نوع الملف المحدد.

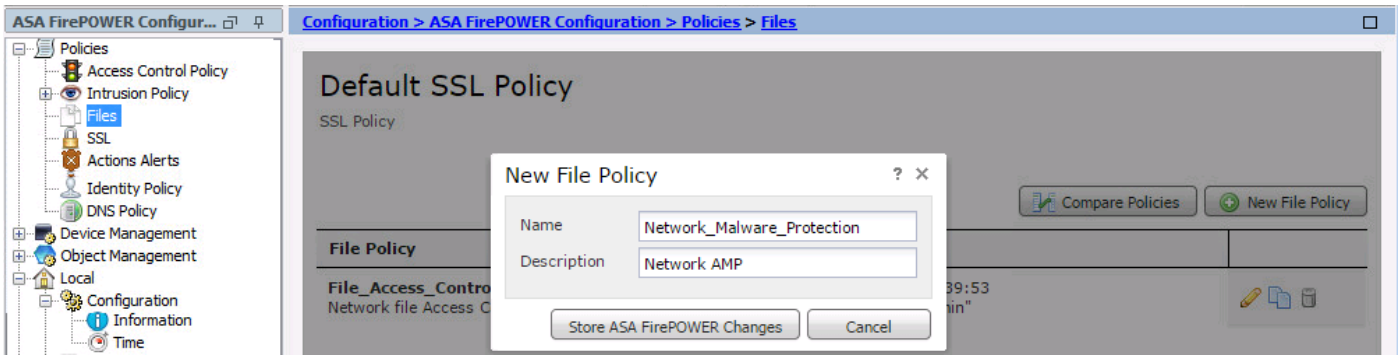
أختر **تخزين تغييرات ASA FirePOWER** لحفظ التكوين.



تكوين حماية البرامج الضارة بالشبكة (AMP)

سجل الدخول إلى ASDM وانتقل إلى **التكوين > ASA Firepower Configuration > السياسات > الملفات.** تظهر صفحة "نهج الملف". الآن انقر على شاشة نهج الملف الجديد التي تظهر.

أدخل **اسم ووصف** إختياري للنهج الجديد، ثم انقر فوق الخيار **Store ASA FirePOWER Changes**. تظهر صفحة قواعد نهج الملف.



انقر فوق خيار **إضافة قاعدة ملف** لإضافة قاعدة لنهج الملف. تمنحك قاعدة الملفات التحكم متعدد المستويات في أنواع الملفات التي تريد تسجيلها أو حظرها أو مسحها ضوئيا بحثا عن برامج ضارة.

بروتوكول التطبيق: حدد أي بروتوكول (افتراضي) أو بروتوكول محدد (HTTP و SMTP و IMAP و POP3 و FTP و SMB)

إتجاه النقل: حدد إتجاه نقل الملف. يمكن أن يكون أي أو تحميل/ تنزيل استنادا إلى بروتوكول التطبيق. يمكنك فحص البروتوكول (HTTP و IMAP و POP3 و FTP و SMB) لتنزيل الملفات والبروتوكول (HTTP و SMTP و FTP و SMB) لتحميل الملفات. أستخدم **أي** خيار لاكتشاف الملفات عبر بروتوكولات تطبيق متعددة، بغض النظر عن المستخدمين الذين يقومون بإرسال الملف أو إستقباله.

الإجراء: بالنسبة لوظيفة حماية البرامج الضارة بالشبكة، يكون الإجراء إما **البحث عن مجموعة البرامج الضارة** أو **حظر البرامج الضارة**. ينتج **البحث عن سحابة البرامج الضارة**

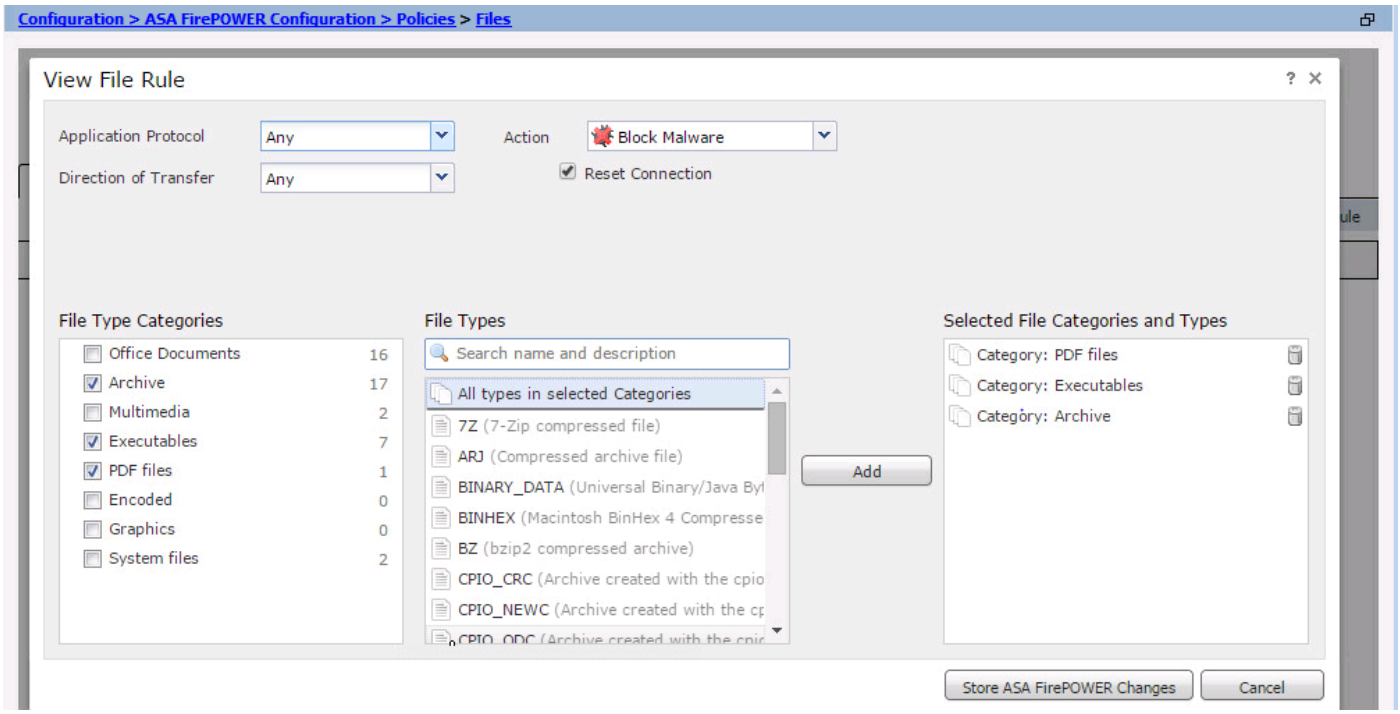
للإجراء حدثا فقط في حين أن **البرامج الضارة لكتلة** الإجراء تقوم بإنشاء الحدث بالإضافة إلى حظر إرسال ملف البرامج الضارة.

> **ملاحظة: يسمح البحث عن مجموعة البرامج الضارة وقواعد الحظر للبرامج الضارة لـ Firepower بحساب تجزئة SHA-256 وإرسالها لعملية البحث في مجموعة النظراء لتحديد ما إذا كانت الملفات التي تجتاز الشبكة تحتوي على برامج ضارة.**

فئات نوع الملف: حدد فئات الملف المحددة.

أنواع الملفات: حدد **أنواع الملفات** المحددة لمزيد من أنواع الملفات متعددة المستويات.

أختر خيار **تخزين تغييرات ASA FirePOWER** لحفظ التكوين.

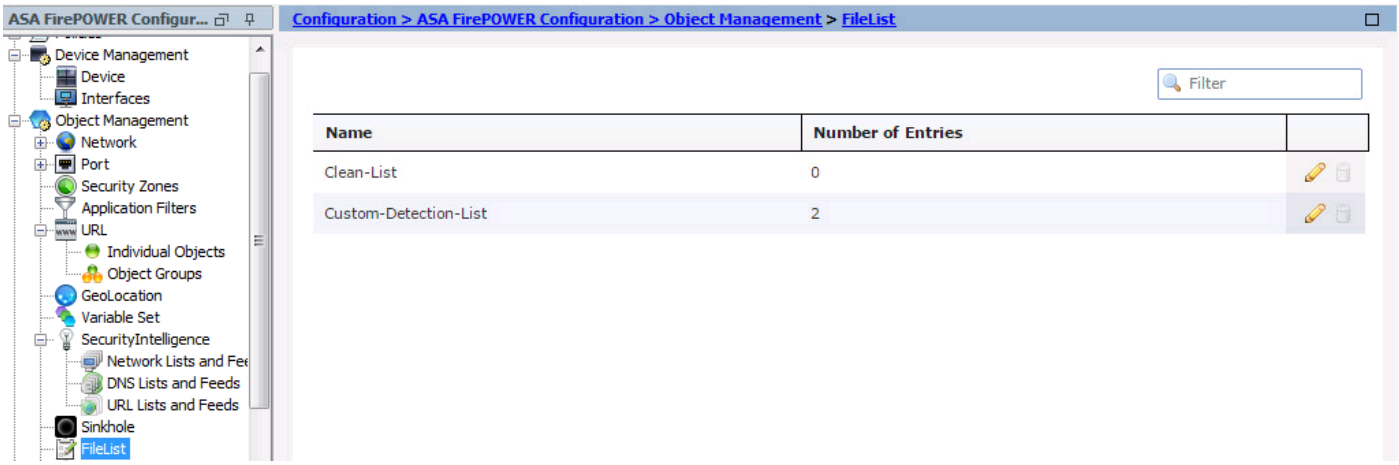


> **ملاحظة**: تعالج نهج الملفات الملفات الملفات بترتيب القاعدة-الإجراء التالي: يعطي الحظر الأولوية على فحص البرامج الضارة، مما يعطي الأسبقية على مجرد الكشف والتسجيل.

إذا قمت بتكوين الحماية المتقدمة من البرامج الضارة المستندة إلى الشبكة (AMP)، وقيام Cisco Cloud باكتشاف المصير النهائي للملف بشكل غير صحيح، فيمكنك إضافة الملف إلى قائمة الملفات باستخدام قيمة تجزئة SHA-256 لتحسين اكتشاف المصير النهائي للملفات في المستقبل. حسب نوع قائمة الملفات، يمكنك القيام بما يلي:

- لمعالجة ملف كما لو كانت السحابة تحدد مصير نهائي نظيف، قم بإضافة الملف إلى القائمة النظيفة.
- لمعالجة ملف كما لو كانت السحابة تحدد خاصية برنامج ضار، قم بإضافة الملف إلى القائمة المخصصة.

لتكوين هذا، انتقل إلى **التكوين > ASA FirePOWER Configuration > Object Management > File List** وتحرير القائمة لإضافة SHA-256.



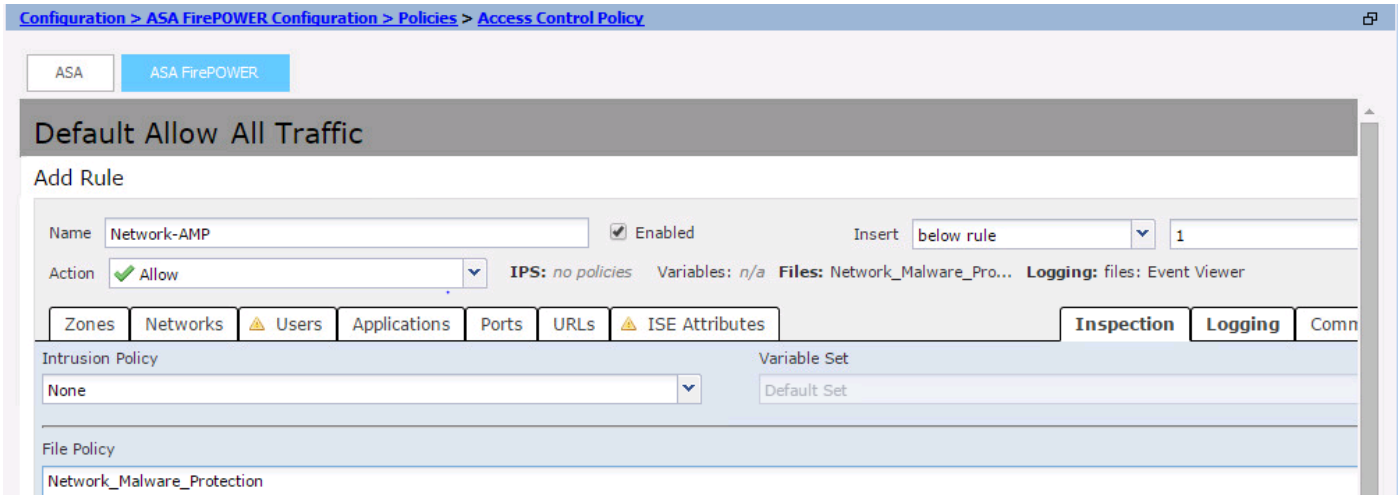
تكوين نهج التحكم بالوصول لنهج الملف

انتقل إلى **التكوين** > ASA Firepower Configuration > **السياسات** > **سياسة التحكم في الوصول**، وقم بإنشاء إما **قاعدة وصول** جديدة أو تحرير **قاعدة الوصول** الموجودة، كما هو موضح في هذه الصورة.

لتكوين نهج الملف، يجب أن يكون الإجراء **يسمح**. انتقل إلى علامة التبويب **فحص**، وحدد **نهج الملف** من القائمة المنسدلة.

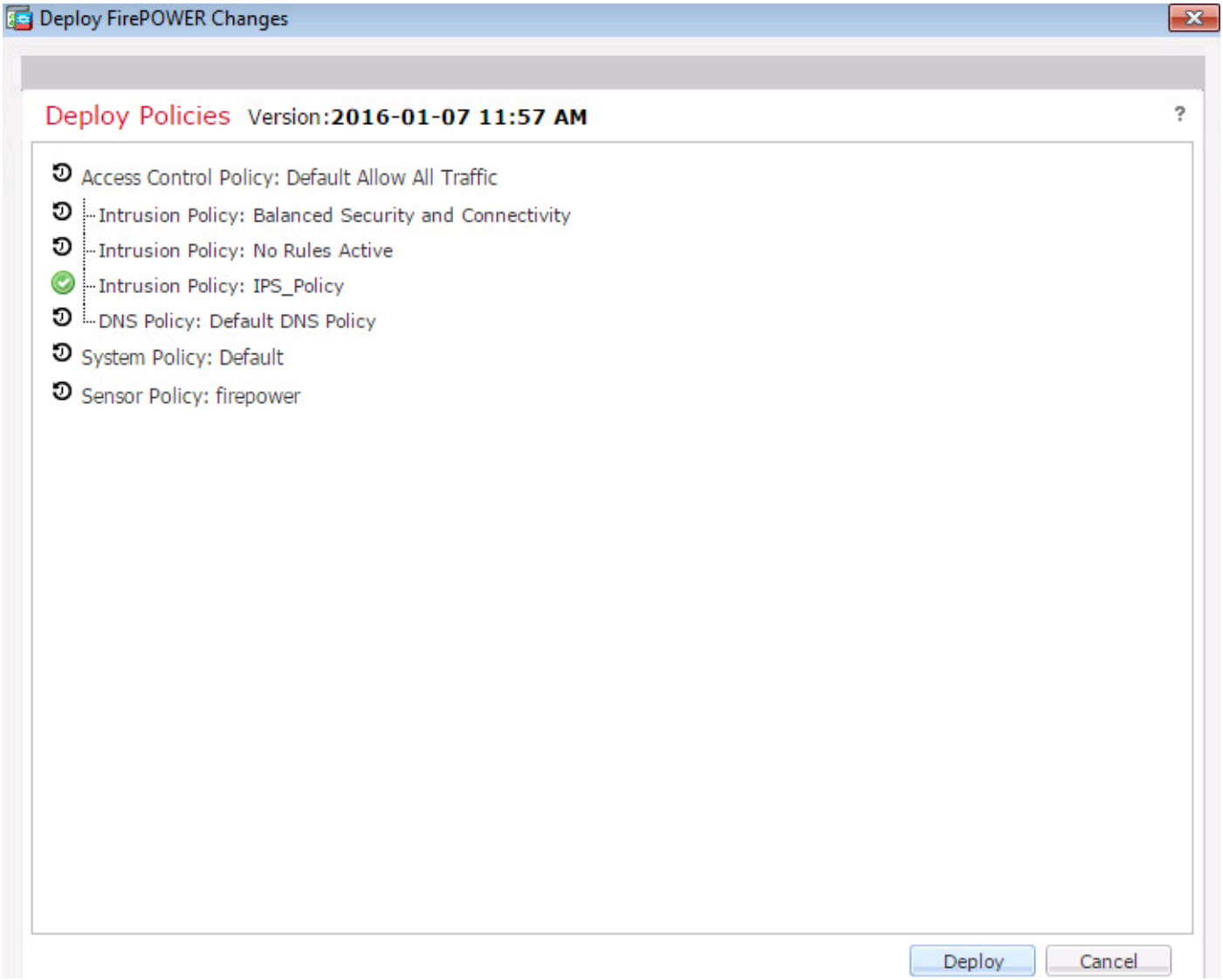
لتمكين التسجيل، انتقل إلى خيار **التسجيل**، وحدد الخيار تسجيل **وملفات السجل** المناسب. انقر فوق زر **حفظ/إضافة** لحفظ التكوين.

أختر خيار **تخزين تغييرات ASA FirePOWER** لحفظ تغييرات سياسة التياز المتردد.



سياسة التحكم بالوصول إلى النشر

انتقل إلى خيار **النشر** ل ASDM، واختر **نشر خيار تغيير FirePOWER** من القائمة المنسدلة. انقر فوق خيار **النشر** لنشر التغييرات.

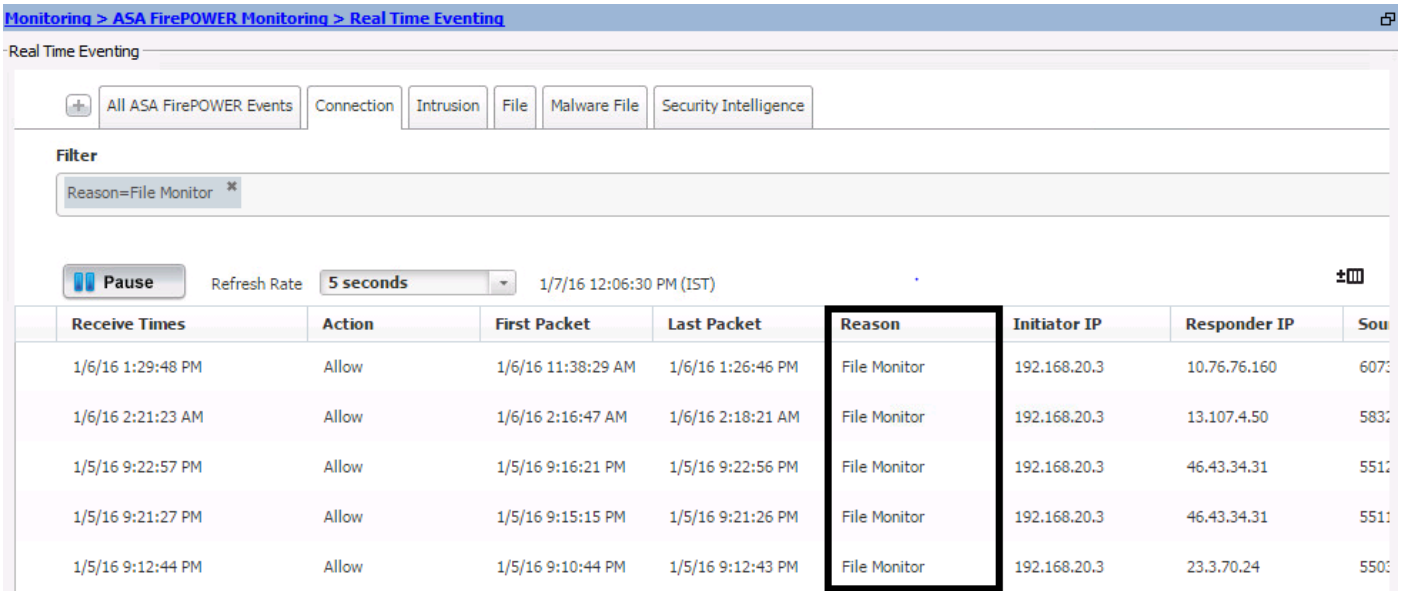


انتقل إلى **المراقبة > مراقبة ASA FirePOWER > حالة المهمة.** تأكد من إكمال المهمة لتطبيق تغيير التكوين.

> **ملاحظة**: في الإصدار 5.4.x، لتطبيق سياسة الوصول على المستشعر، يلزمك **النقر فوق تطبيق تغييرات ASA FirePOWER.**

مراقبة الاتصال لأحداث نهج الملف

لعرض الأحداث التي تم إنشاؤها بواسطة وحدة FirePOWER النمطية المرتبطة بنهج الملف، انتقل إلى **المراقبة > مراقبة ASA FirePOWER > التدقيق في الوقت الفعلي.**



التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

تأكد من أن نهج الملف تم تكوينه بشكل صحيح مع أنواع البروتوكول/ الإتجاه/ الإجراء/ الملفات. تأكد من تضمين نهج الملف الصحيح في قواعد الوصول.

تأكد من اكتمال نشر نهج التحكم بالوصول بنجاح.

مراقبة أحداث الاتصال وأحداث الملفات (**المراقبة > مراقبة ASA FirePOWER > التصحيح في الوقت الفعلي**) للتحقق مما إذا كان تدفق حركة المرور يصل إلى القاعدة الصحيحة أم لا.

معلومات ذات صلة

- [الدعم التقني والمستندات - Cisco Systems]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).