

Configure el módulo de FirePOWER para la red AMP o el control de archivos con el ASDM.

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configure la directiva del archivo para el /Network AMP del control de archivos](#)

[Configure el control de acceso del archivo](#)

[Configure la protección de Malware de la red \(red el AMP\)](#)

[Configure la directiva del control de acceso para la directiva del archivo](#)

[Despliegue la directiva del control de acceso](#)

[Monitoree la conexión para los eventos de la directiva del archivo](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe las funciones avanzadas red del control de acceso de la protección de Malware (AMP) /file del módulo de FirePOWER y del método para configurarlos con el Administrador de dispositivos de seguridad adaptante (ASDM).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del Firewall adaptante y del ASDM del dispositivo de seguridad (ASA).
- Conocimiento del dispositivo de FirePOWER.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de software corriente 5.4.1 de los módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) y posterior.
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) esa versión de software 6.0.0 del funcionamiento y posterior.

- ASDM 7.5.1 y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El software/el malware malévolo puede ingresar en la red de una organización vía las diferentes formas. Para identificar y atenuar los efectos de este software y malware malévolo, las características AMP de FirePOWER se pueden utilizar para detectar y bloquear opcionalmente la transmisión del software y del malware malévolo en la red.

Con las funciones del control de archivos, usted puede elegir monitorear (detectar), bloquear, o permitir la transferencia de File Upload (Subir archivo) y la descarga. Por ejemplo, una directiva del archivo puede ser implementada que bloquea la descarga de los archivos ejecutables del usuario.

Con las funciones de la red AMP, usted puede seleccionar los tipos de archivo que usted desea monitorear sobre los protocolos de uso general y enviar SHA 256 desmenuza, los meta datos de los archivos, o aún las copias de los archivos ellos mismos a la nube de la inteligencia del Cisco Security para el análisis del malware. La disposición de las devoluciones de la nube para el archivo desmenuza como limpio o malévolo basado en el análisis del archivo.

El control de archivos y el AMP para FirePOWER se pueden configurar como directiva del archivo y utilizar como parte de su configuración total del control de acceso. Las directivas del archivo asociadas a las reglas del control de acceso examinan el tráfico de la red que cumple las condiciones de la regla.

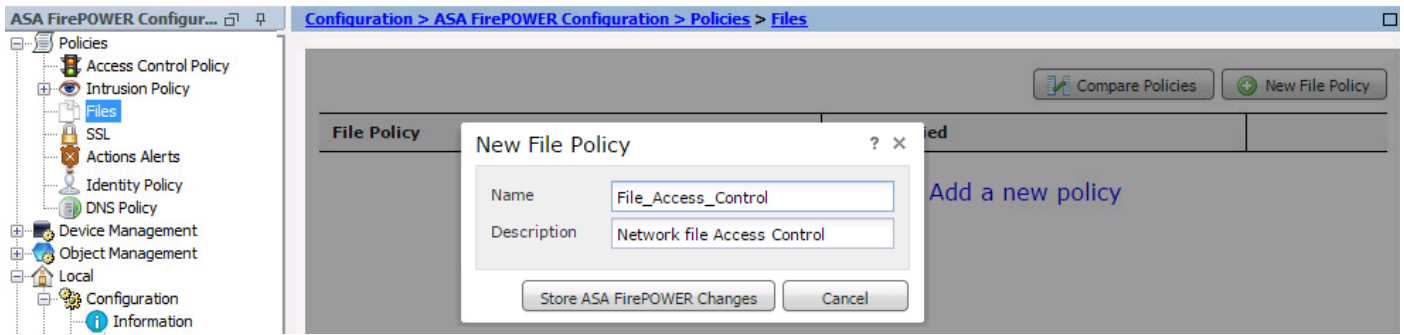
Note: Asegúrese de que el módulo de FirePOWER tenga una licencia de la protección/del control/de Malware para configurar estas funciones. Para verificar las licencias, elija la **configuración > la configuración > la licencia ASA FirePOWER**.

Configure la directiva del archivo para el /Network AMP del control de archivos

Configure el control de acceso del archivo

Inicie sesión al ASDM y elija la **configuración > la configuración > las directivas > los archivos ASA FirePOWER**. El cuadro de diálogo de la **directiva del nuevo archivo** aparece.

Ingrese un nombre y una descripción opcional para su nueva directiva, después haga clic la opción de los **cambios del almacén ASA FirePOWER**. La página de la regla de la directiva del archivo aparece.



El tecleo **agrega la regla del archivo** para agregar una regla a la directiva del archivo. La regla del archivo le da el control granular sobre los tipos de archivo que usted quiere registrar, bloquear, o analizar para el malware.

Application Protocol: Especifique el Application Protocol como (valor por defecto) o el protocolo específico (HTTP, S TP, IMAP, POP3, FTP, SMB).

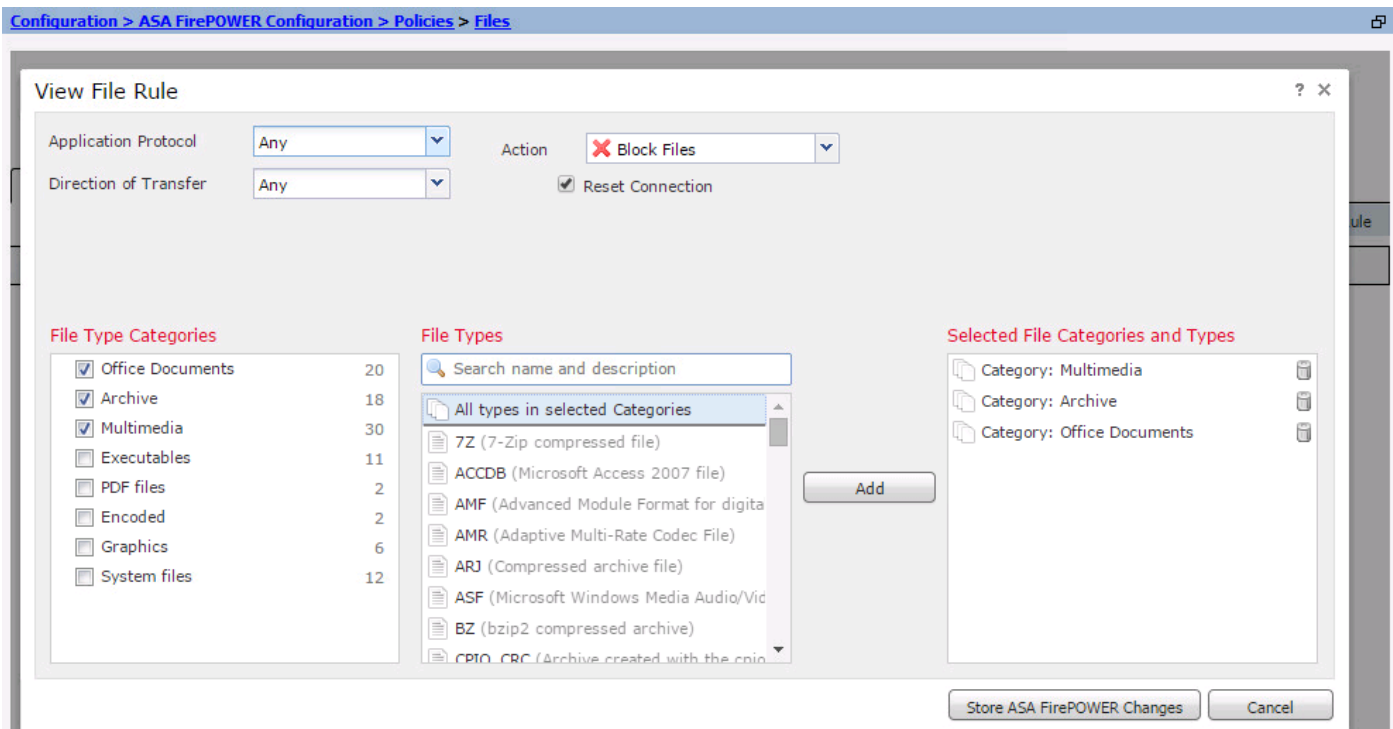
Dirección de la transferencia: Especifique la dirección de la transferencia de archivos. Podía ser ninguno o carga/descarga basada en el Application Protocol. Usted puede examinar el protocolo (HTTP, IMAP, POP3, FTP, SMB) para saber si hay la descarga del archivo y el protocolo (HTTP, S TP, FTP, SMB) para File Upload (Subir archivo). Utilice la **cualquier** opción para detectar los archivos sobre los protocolos de la aplicación múltiple, sin importar si los usuarios envían o reciben el archivo.

Acción: Especifique la acción para las funciones del control de acceso del archivo. La acción sería **detecta los archivos** o **bloquea los archivos**. **Detecte la** acción del **archivo** genera el evento y la acción de los **archivos del bloque** genera el evento y bloquea la transmisión de archivo. Con la acción de los **archivos del bloque**, usted puede seleccionar opcionalmente **para reajustar la conexión** para terminar la conexión.

Categorías del tipo de archivo: Seleccione las categorías del tipo de archivo para las cuales usted quiere al archivo del bloque o genera la alerta.

Tipos de archivo: Seleccione los tipos de archivo. La opción de los tipos de archivo da una opción más granular para elegir el tipo de archivo específico.

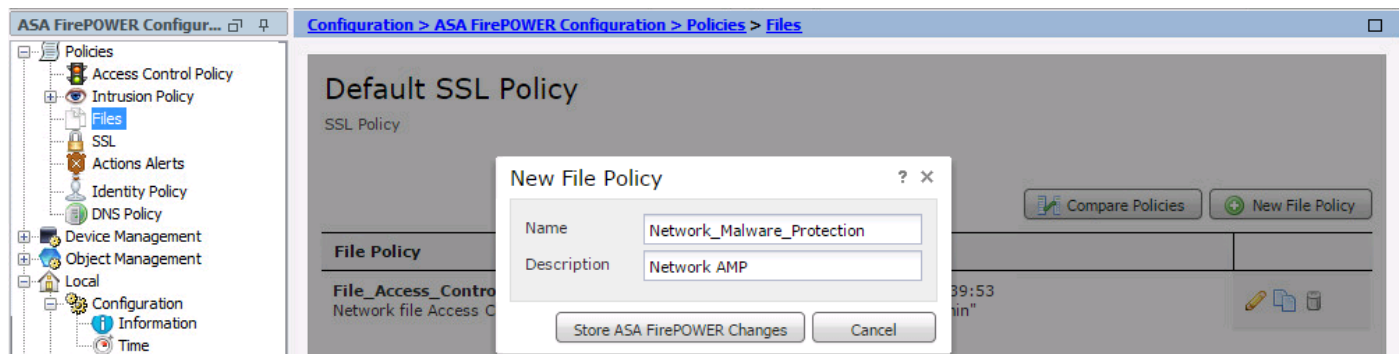
Elija la opción de los **cambios del almacén ASA FirePOWER** para salvar la configuración.



Configure la protección de Malware de la red (red el AMP)

Inicie sesión al ASDM y navegue a la **configuración > a la configuración > a las directivas > a los archivos ASA FirePOWER**. La página de la directiva del archivo aparece. Ahora haga clic en el cuadro de diálogo de la directiva del nuevo archivo aparece.

Ingrese un **nombre** y una descripción opcional para su nueva directiva, después haga clic en la opción de los **cambios del almacén ASA FirePOWER**. La página de las reglas de la directiva del archivo aparece.



Haga clic la opción de la **regla del archivo del agregar** para agregar una regla para clasificar la directiva. La regla del archivo le da el control granular sobre los tipos de archivo que usted quiere registrar, bloquear, o analizar para el malware.

Application Protocol: Especifique ningunos (predeterminado) o el protocolo específico (HTTP, S TP, IMAP, POP3, FTP, el SMB)

Dirección de la transferencia: Especifique la dirección de la transferencia de archivos. Podía ser ninguno o descarga de la carga por teletratamiento basada en el Application Protocol. Usted puede examinar el protocolo (HTTP, IMAP, POP3, FTP, SMB) para saber si hay descarga del archivo y el protocolo (HTTP, S TP, FTP, SMB) para File Upload (Subir archivo). Utilice **cualquier** opción para detectar los archivos sobre los protocolos de la aplicación múltiple, sin importar los usuarios que envían o que reciben el archivo.

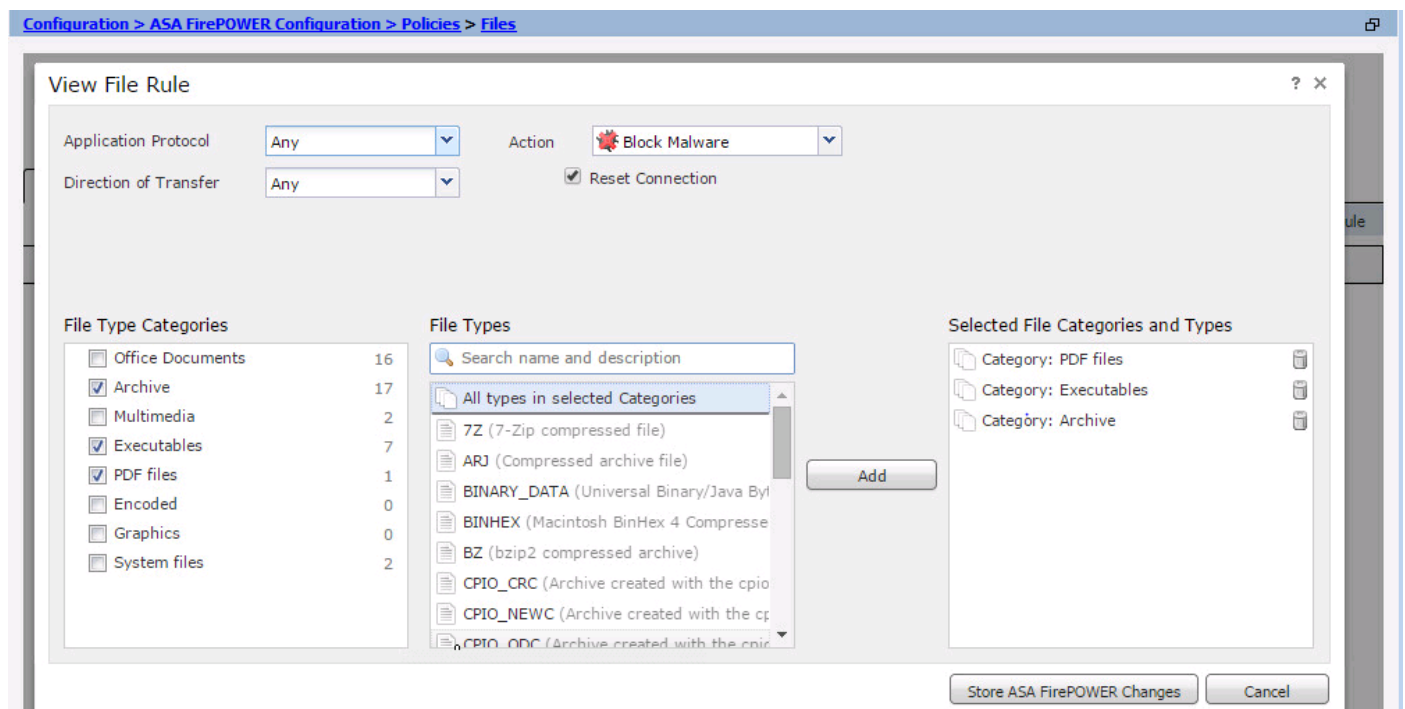
Acción: Para las funciones de la protección de Malware de la red, la acción sería cualquier **operaciones de búsqueda de la nube de Malware** o **bloquearía Malware**. Las **operaciones de búsqueda de la nube de Malware** de la acción generan solamente un evento mientras que el **bloque Malware** de la acción genera el evento así como bloquean la transmisión de archivo del malware.

Note: Las reglas de **Malware del andBlock** de las **operaciones de búsqueda de la nube de Malware** permiten que FirePOWER calcule el hash del SHA-256 y lo envíe para que el proceso de búsqueda de la nube determine si los archivos que atraviesan la red contienen el malware.

Categorías del tipo de archivo: Seleccione las categorías del archivo específico.

Tipos de archivo: Seleccione los **tipos de archivo** específico para tipos de archivo más granulares.

Elija los **cambios del almacén ASA FirePOWER** de la opción para salvar la configuración.

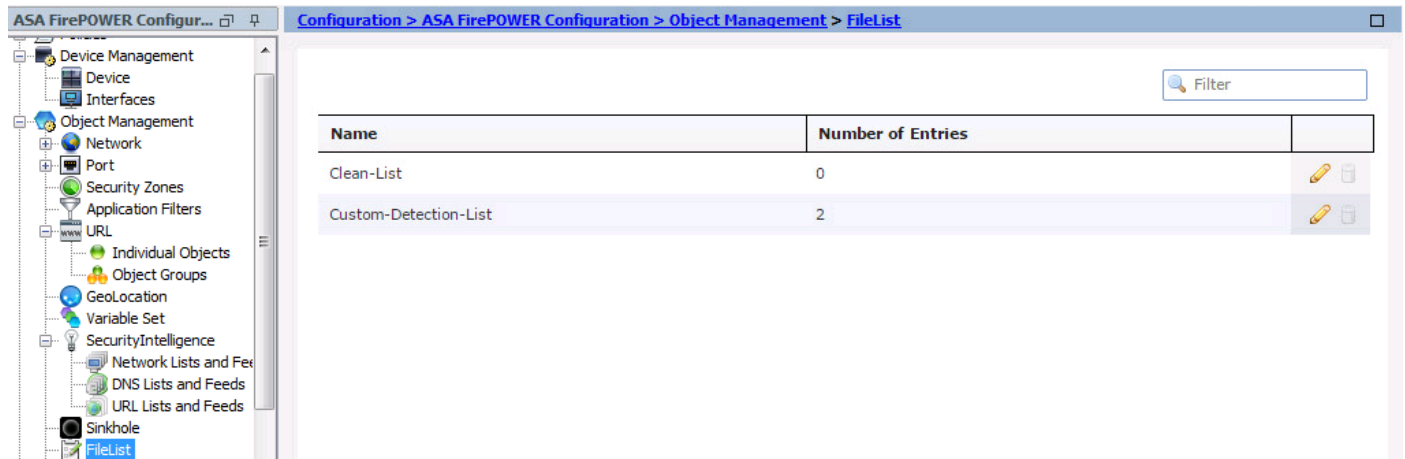


Note: Las directivas del archivo manejan los archivos en la orden siguiente de la regla- acción: El bloqueo toma la precedencia sobre el examen del malware, que toma la precedencia sobre la detección y el registro simples.

Si usted configura la protección avanzada network basado del malware (AMP), y nube de Cisco detecta incorrectamente la disposición de un archivo, usted puede agregar el archivo a la lista de archivos usando un valor de troceo del SHA-256 para mejorar detecta la disposición del archivo en el futuro. dependiendo del tipo de lista de archivos, usted puede hacer:

- Para tratar un archivo como si la nube asignara una disposición limpia, agregue el archivo a la lista limpia.
- Para tratar un archivo como si la nube asignara una disposición del malware, agregue el archivo a la lista de encargo.

Para configurar esto, navegue a la configuración > a la configuración ASA FirePOWER > a la Administración > a la lista de archivos del objeto y edite la lista para agregar el SHA-256.



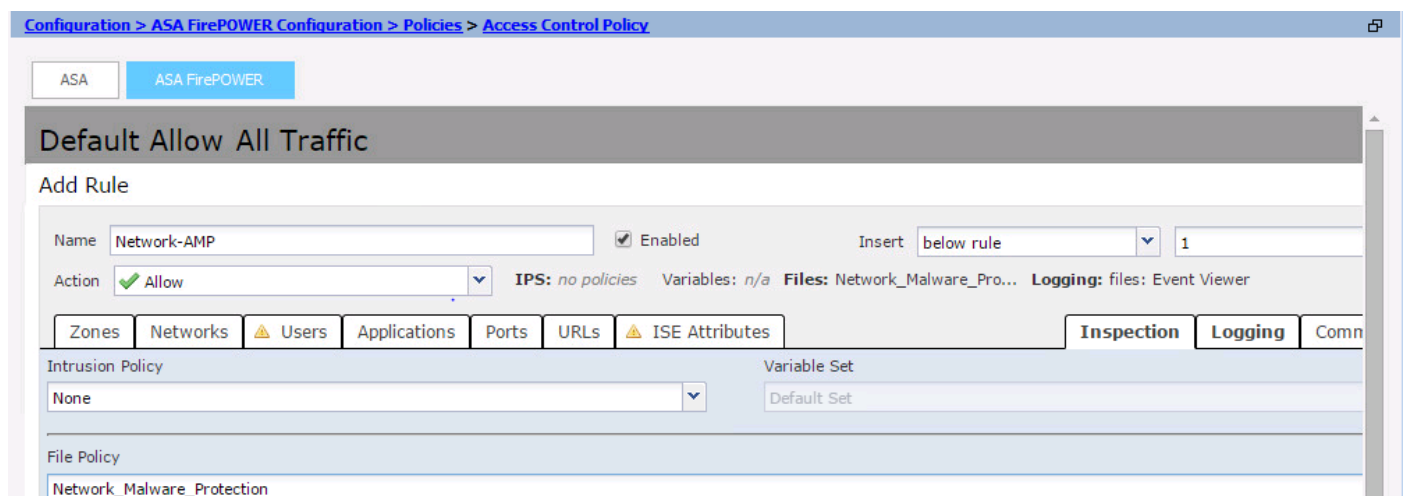
Configure la directiva del control de acceso para la directiva del archivo

Navegue a la configuración > a la configuración ASA FirePOWER > a las directivas > a la directiva del control de acceso, y cree cualquier nueva regla de acceso o edite la regla de acceso existente, tal y como se muestra en de esta imagen.

Para configurar la directiva del archivo, la acción debe ser **permite**. Navegue a la lengüeta del **examen**, y seleccione la **directiva del archivo del** menú desplegable.

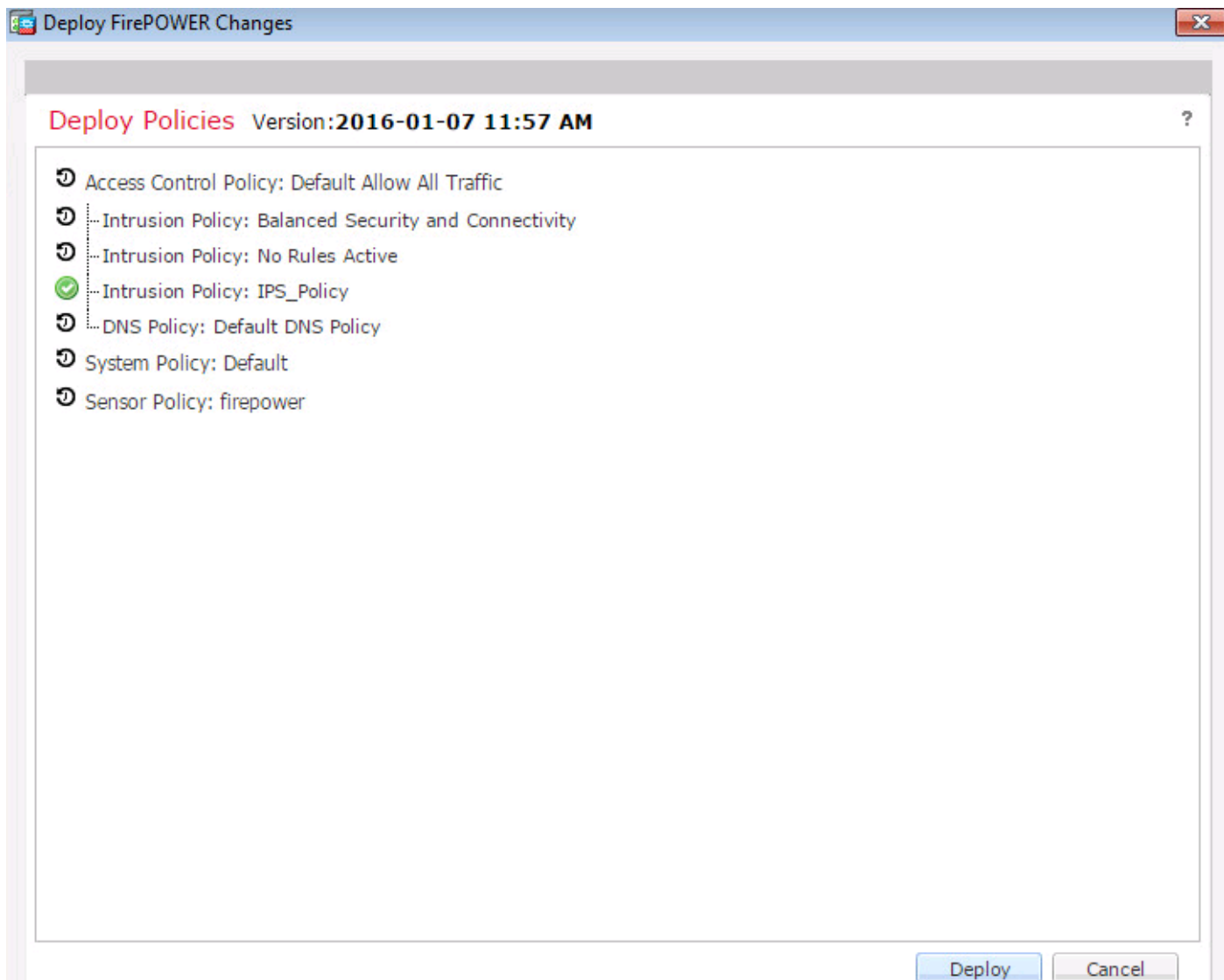
Para habilitar el registro, navegue la **opción de registro**, y seleccione la opción de registro y la opción apropiadas de los **archivos del registro**. Haga clic la **salvaguardia/el botón Add** para salvar la configuración.

Elija los **cambios del almacén ASA FirePOWER de la** opción para salvar los cambios de política AC.



Despliegue la directiva del control de acceso

Navegue a ASDM despliegan la opción, y eligen despliegan la opción del cambio de FirePOWER del menú desplegable. Haga clic en **despliegan la** opción para desplegar los cambios.



Navegue a **monitorear > ASA FirePOWER que monitorea > estatus de la tarea**. Asegúrese de que la tarea deba completar para aplicar el cambio de configuración.

Note: En la versión 5.4.x, aplicar la política de acceso al sensor, usted necesita clickApply los **cambios ASA FirePOWER**.

Conexión del monitor para los eventos de la directiva del archivo

Para ver los eventos generados por el módulo de FirePOWER relacionado para clasificar la directiva, navegue a **monitorear > ASA FirePOWER que monitorea > Eventing en tiempo real**.

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

All ASA FirePOWER Events | Connection | Intrusion | File | Malware File | Security Intelligence

Filter
Reason=File Monitor ✕

Pause Refresh Rate 5 seconds 1/7/16 12:06:30 PM (IST)

Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP	Sou
1/6/16 1:29:48 PM	Allow	1/6/16 11:38:29 AM	1/6/16 1:26:46 PM	File Monitor	192.168.20.3	10.76.76.160	6073
1/6/16 2:21:23 AM	Allow	1/6/16 2:16:47 AM	1/6/16 2:18:21 AM	File Monitor	192.168.20.3	13.107.4.50	5833
1/5/16 9:22:57 PM	Allow	1/5/16 9:16:21 PM	1/5/16 9:22:56 PM	File Monitor	192.168.20.3	46.43.34.31	5511
1/5/16 9:21:27 PM	Allow	1/5/16 9:15:15 PM	1/5/16 9:21:26 PM	File Monitor	192.168.20.3	46.43.34.31	5511
1/5/16 9:12:44 PM	Allow	1/5/16 9:10:44 PM	1/5/16 9:12:43 PM	File Monitor	192.168.20.3	23.3.70.24	5503

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Asegúrese de que la directiva del archivo configurado correctamente con los tipos de archivo de la acción de la dirección del protocolo. Asegure a eso la directiva correcta del archivo incluida en las reglas de acceso.

Asegúrese de que la implementación de política del control de acceso complete con éxito.

Monitoree los eventos de los eventos de conexión y del archivo (**supervisión > ASA FirePOWER que monitorea > Eventing en tiempo real**) para verificar si el flujo de tráfico está golpeando la regla correcta o no.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)