Configurare il modulo FirePOWER per Network AMP o il controllo file con ASDM.

Sommario

Introduzione

Questo documento descrive la funzionalità Network Advanced Malware Protection (AMP)/file access control del modulo FirePOWER e il metodo per configurarli con Adaptive Security Device Manager (ASDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del firewall ASA (Adaptive Security Appliance) e di ASDM.
- Conoscenza dell'appliance FirePOWER.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA Firepower Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 5.4.1 e successive.
- Modulo ASA Firepower (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software versione 6.0.0 e successive.

- ASDM 7.5.1 e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Software dannoso o malware può entrare nella rete di un'organizzazione in diversi modi. Al fine di identificare e mitigare gli effetti di questo software dannoso e malware, le funzionalità AMP di FirePOWER possono essere utilizzate per rilevare e facoltativamente bloccare la trasmissione di software dannoso e malware nella rete.

Con la funzionalità di controllo dei file, è possibile scegliere di monitorare (rilevare), bloccare o consentire il trasferimento del caricamento e del download dei file. Ad esempio, è possibile implementare un criterio di file che blocca il download di file eseguibili da parte dell'utente.

Con la funzionalità Network AMP, è possibile selezionare i tipi di file che si desidera monitorare nei protocolli di uso comune e inviare hash SHA 256, metadati dai file o persino copie dei file stessi a Cisco Security Intelligence Cloud per l'analisi del malware. Cloud restituisce l'eliminazione degli hash dei file come puliti o dannosi in base all'analisi dei file.

Il controllo dei file e AMP for Firepower possono essere configurati come regole per i file e utilizzati come parte della configurazione generale del controllo degli accessi. I criteri file associati alle regole di controllo di accesso ispezionano il traffico di rete che soddisfa le condizioni delle regole.

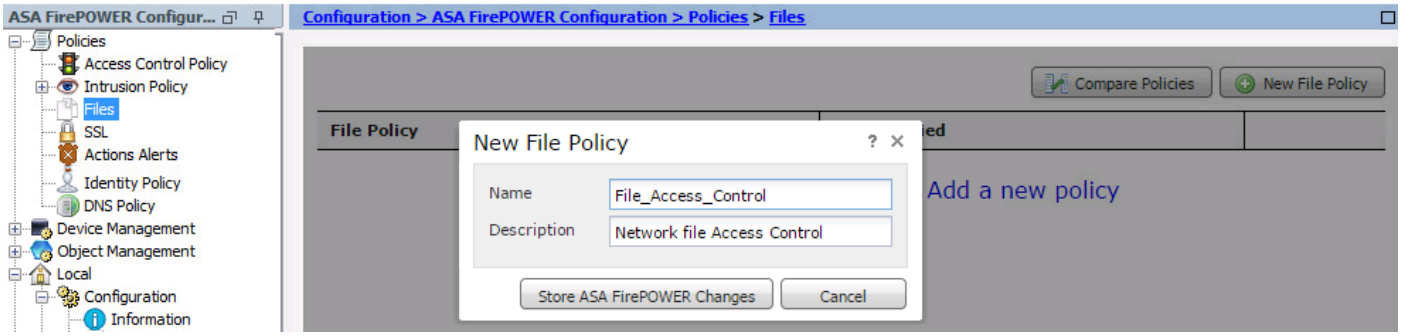
> **Nota:** Per configurare questa funzionalità, verificare che il modulo FirePOWER disponga di una licenza Protect/Control/Malware. Per verificare le licenze, scegliere **Configurazione > ASA FirePOWER Configuration > Licenza.**

Configurare i criteri file per Controllo file/AMP di rete

Configura controllo accesso file

Accedere a ASDM e scegliere **Configurazione > Configurazione di ASA Firepower > Criteri > File.** Viene visualizzata la finestra di dialogo **Nuovo criterio file**.

Immettere un nome e una descrizione facoltativa per il nuovo criterio, quindi fare clic su **Archivia ASA Firepower Changes** option (Archivia ASA Firepower Changes). Viene visualizzata la pagina Regola dei criteri per i file.



Per aggiungere una regola al criterio file, fare clic su **Aggiungi regola file**. La regola file offre il controllo granulare sui tipi di file che si desidera registrare, bloccare o analizzare per rilevare malware.

Protocollo applicazione: Specificare il protocollo dell'applicazione come Any (predefinito) o il protocollo specifico (HTTP, SMTP, IMAP, POP3, FTP, SMB).

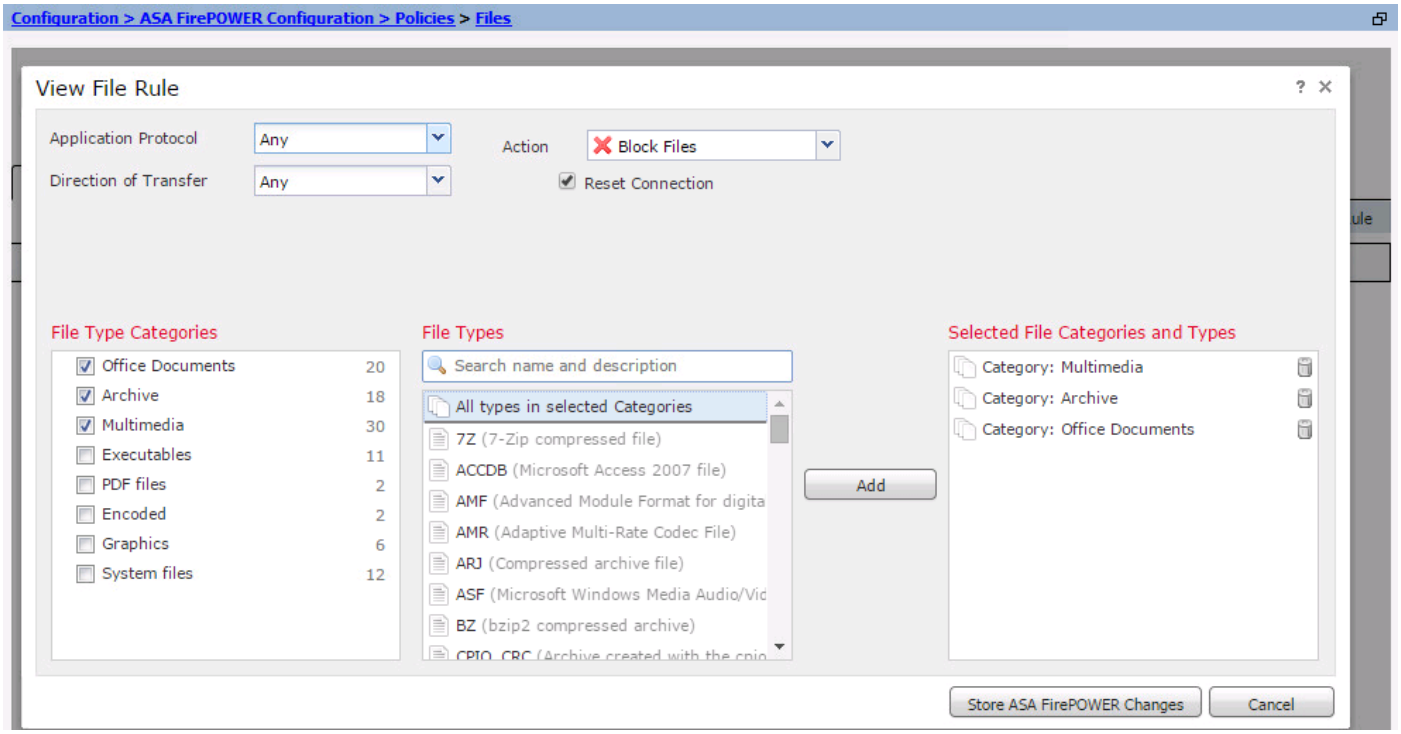
Direzione trasferimento: Specificare la direzione del trasferimento file. Può essere Any o Upload/Download in base al protocollo dell'applicazione. È possibile controllare il protocollo (HTTP, IMAP, POP3, FTP, SMB) per il download dei file e il protocollo (HTTP, SMTP, FTP, SMB) per il caricamento dei file. Utilizzare l'opzione **Any** per rilevare i file su più protocolli applicativi, indipendentemente dal fatto che gli utenti inviino o ricevano il file.

Azione: Specificare l'azione per la funzionalità Controllo accesso file. L'azione può essere **Rileva file** o **Blocca file. L'**azione **Rileva file** genera l'evento e l'azione **Blocca file** genera l'evento e blocca la trasmissione dei file. Con l'azione **Blocca file**, è possibile selezionare facoltativamente **Reimposta connessione** per terminare la connessione.

Categorie di tipi di file: selezionare le categorie di tipi di file per le quali si desidera bloccare il file o generare l'avviso.

Tipi di file: Selezionare i tipi di file. L'opzione Tipi di file offre un'opzione più granulare per scegliere il tipo di file specifico.

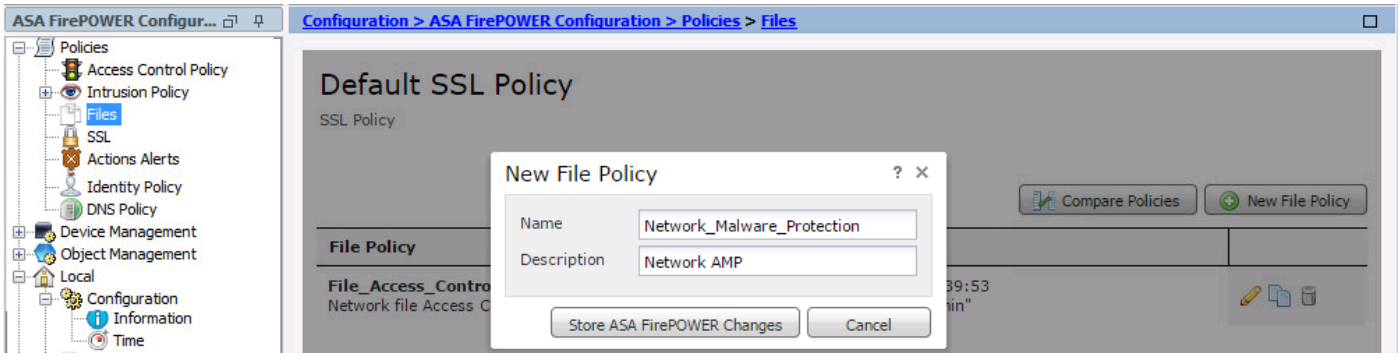
Selezionare l'opzione **Store ASA Firepower Changes** per salvare la configurazione.



Configurare Network Malware Protection (Network AMP)

Accedere a ASDM e selezionare **Configurazione > ASA Firepower Configuration > Policy > File.** Viene visualizzata la pagina Criterio file. Fare clic su. Viene visualizzata la finestra di dialogo Nuovo criterio file.

Immettere un **nome** e una **descrizione** facoltativa per il nuovo criterio, quindi fare clic sull'opzione **Store ASA Firepower Changes**. Viene visualizzata la pagina Regole dei criteri del file.



Fare clic sull'opzione **Aggiungi regola file** per aggiungere una regola al criterio file. La regola file offre il controllo granulare sui tipi di file che si desidera registrare, bloccare o analizzare per rilevare malware.

Protocollo applicazione: Specificare Any (predefinito) o un protocollo specifico (HTTP, SMTP, IMAP, POP3, FTP, SMB)

Direzione trasferimento: Specificare la direzione del trasferimento file. Può essere Any o Upload/ Download in base al protocollo dell'applicazione. È possibile ispezionare i protocolli (HTTP, IMAP, POP3, FTP, SMB) per il download dei file e i protocolli (HTTP, SMTP, FTP, SMB) per il caricamento dei file. Utilizzare l'opzione **Any** per rilevare i file su più protocolli applicativi, indipendentemente dagli utenti che inviano o ricevono il file.

Azione: Per la funzionalità Protezione da malware di rete, Action può essere **Ricerca cloud**

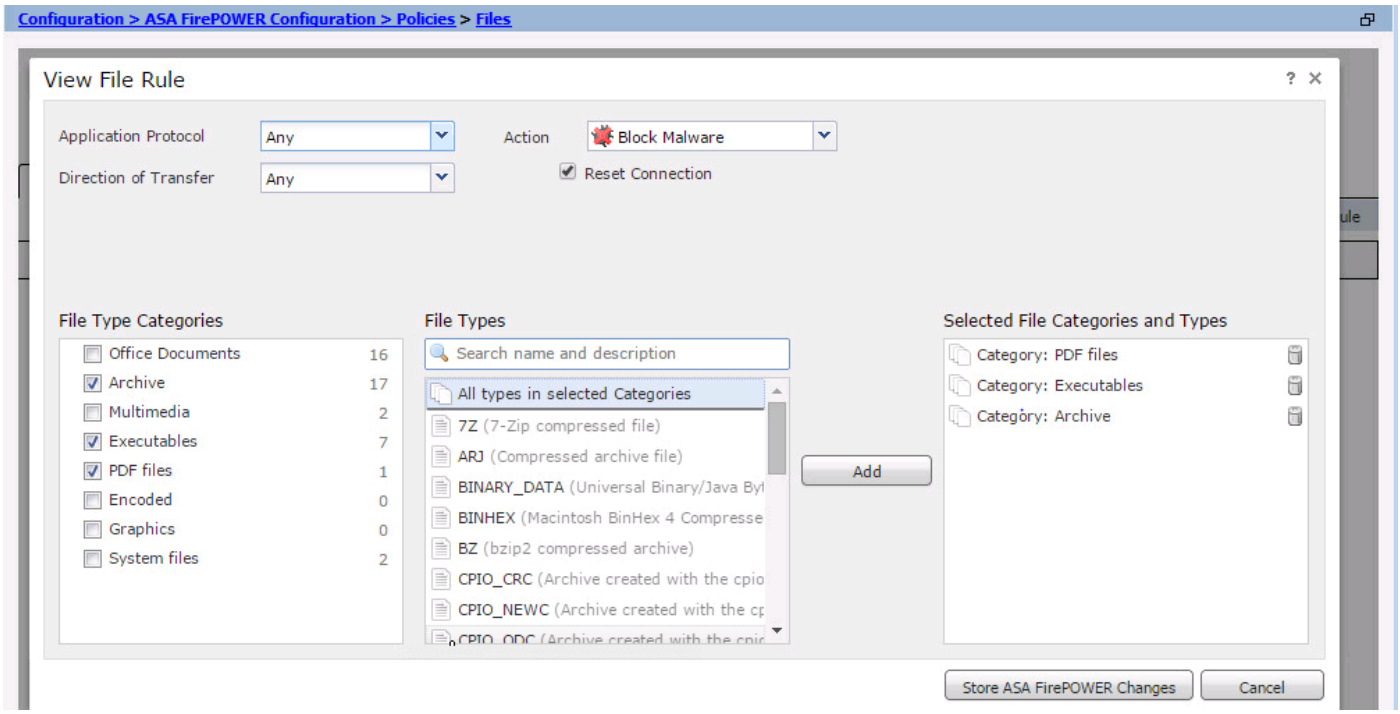
malware o **Blocca malware.** Action **Ricerca cloud malware** genera solo un evento, mentre action **Blocca malware** genera l'evento e blocca la trasmissione del file malware.

> **Nota: Le** regole **Malware Cloud Lookup e Block Malware** consentono a Firepower di calcolare l'hash SHA-256 e di inviarlo per il processo di ricerca cloud per determinare se i file che attraversano la rete contengono malware.

Categorie di tipi di file: selezionare le categorie di file specifiche.

Tipi di file: Selezionare i **tipi di file** specifici per tipi di file più granulari.

Selezionare l'opzione **Store ASA Firepower Changes** per salvare la configurazione.

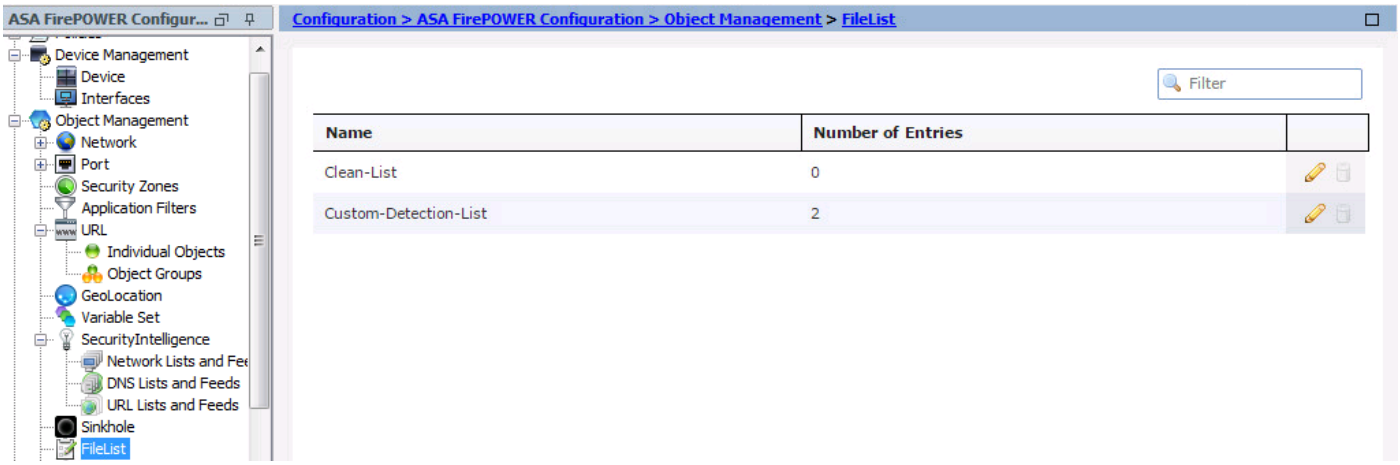


> **Nota:** I criteri file gestiscono i file nell'ordine di azione delle regole seguente: Il blocco ha la precedenza sull'ispezione del malware, che ha la precedenza sul semplice rilevamento e registrazione.

Se si configura AMP (Advanced Malware Protection) basato sulla rete e Cisco Cloud rileva in modo errato la disposizione di un file, è possibile aggiungere il file all'elenco dei file utilizzando un valore hash SHA-256 per migliorare il rilevamento della disposizione del file in futuro. a seconda del tipo di elenco di file, è possibile:

- Per trattare un file come se il cloud avesse assegnato una disposizione pulita, aggiungere il file all'elenco di pulitura.
- Per trattare un file come se il cloud assegnasse una disposizione malware, aggiungere il file all'elenco personalizzato.

Per configurare questa opzione, selezionare **Configurazione > Configurazione ASA FirePOWER > Gestione oggetti > Elenco file** e modificare l'elenco per aggiungere SHA-256.



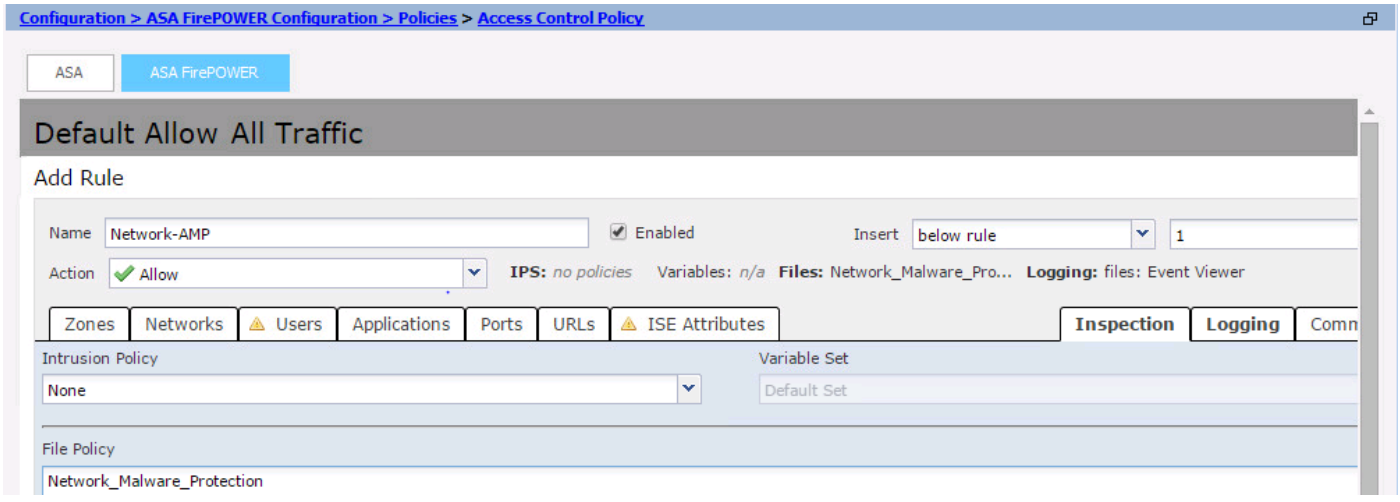
Configura i criteri di controllo di accesso per i criteri file

Selezionare **Configurazione > Configurazione di ASA Firepower > Criteri > Criteri di controllo di accesso** e creare una nuova **regola di accesso** o modificare una **regola di accesso** esistente**,** come mostrato nell'immagine.

Per configurare i criteri file, l'azione deve essere **Consenti**. Passare alla scheda **Ispezione** e selezionare **Criterio file** dal menu a discesa.

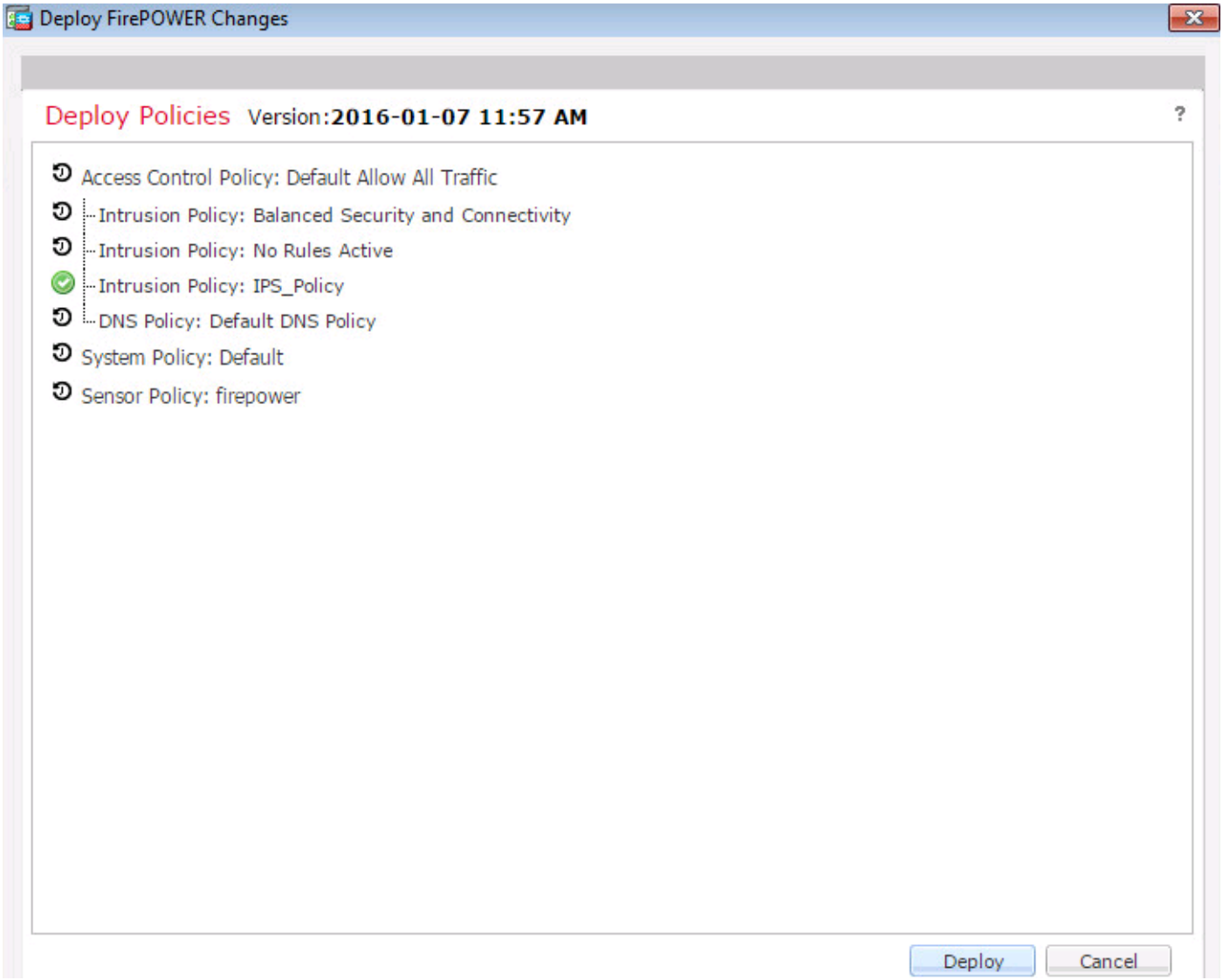
Per abilitare la registrazione, selezionare l'opzione **logging** e selezionare l'opzione di registrazione appropriata e l'opzione **Log Files**. Fare clic sul pulsante **Save/Add** per salvare la configurazione.

Scegliere l'opzione **Store ASA Firepower Changes** per salvare le modifiche ai criteri di CA.



Distribuisci criteri di controllo di accesso

Passare all'opzione **Deploy** di ASDM e scegliere l'opzione **Deploy Firepower Change** dal menu a discesa. Fare clic sull'opzione **Deploy** per distribuire le modifiche.

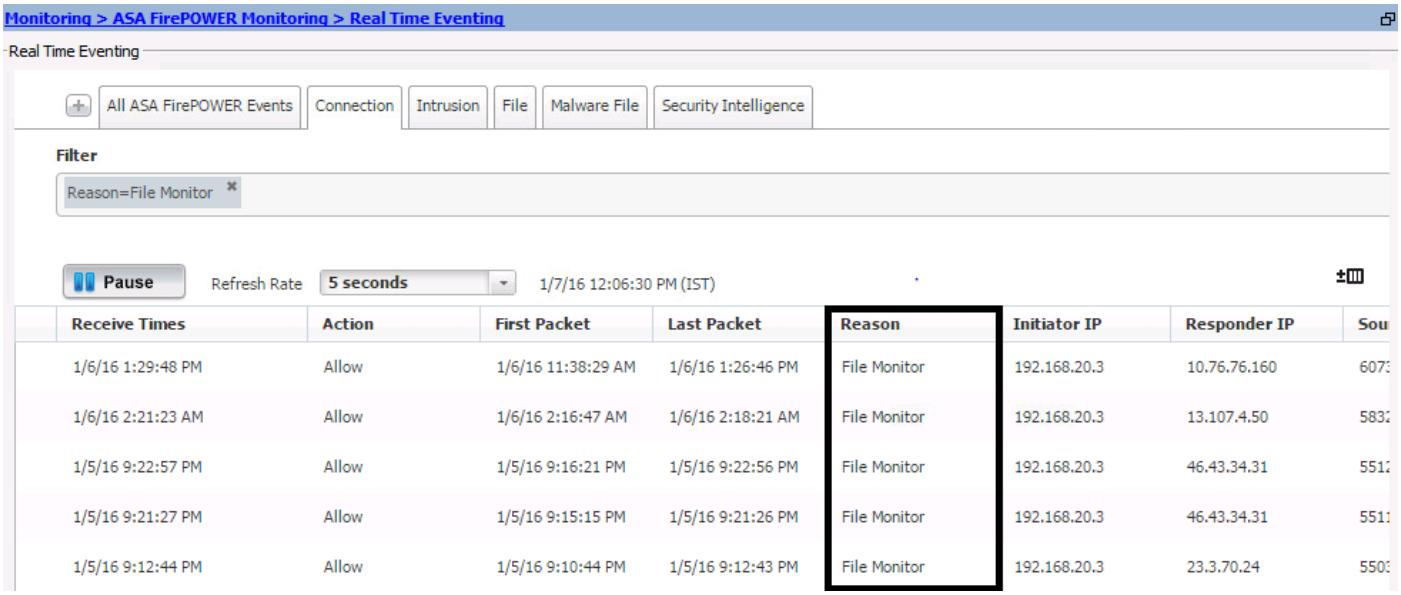


Passare a **Monitoraggio > Monitoraggio ASA Firepower > Stato task. Per** applicare la modifica alla configurazione, verificare che il task debba essere completato.

> **Nota:** Nella versione 5.4.x, per applicare i criteri di accesso al sensore, è necessario **fare clic su Applica modifiche ASA FirePOWER.**

Monitoraggio connessione per eventi di criteri file

Per visualizzare gli eventi generati dal modulo Firepower in relazione alla policy sui file, selezionare **Monitoraggio > Monitoraggio ASA Firepower > Eventi in tempo reale.**



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Verificare che i criteri file siano configurati correttamente con il tipo di file, il tipo di file, il tipo di file, la direzione e l'azione. Verificare che i criteri file corretti siano inclusi nelle regole di accesso.

Verificare che la distribuzione dei criteri di controllo di accesso venga completata correttamente.

Monitorare gli eventi di connessione e file (**Monitoraggio > Monitoraggio di ASA Firepower > Eventi in tempo reale**) per verificare se il flusso di traffico sta raggiungendo la regola corretta.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems