Konfigurieren Sie das FirePOWER-Modul für Netzwerk-AMP oder Dateikontrolle mit ASDM.

Inhalt

Einführung

Dieses Dokument beschreibt die Funktionen für die Netzwerk-AMP-/Dateizugriffskontrolle (Network Advanced Malware Protection) des FirePOWER-Moduls und die Methode, um diese mit dem Adaptive Security Device Manager (ASDM) zu konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis der ASA-Firewall (Adaptive Security Appliance) und des ASDM.
- Fachwissen der FirePOWER-Appliance.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 5.4.1 und höher
- ASA FirePOWER-Modul (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) mit Softwareversion 6.0.0 und höher

- ASDM 7.5.1 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Bösartige Software/Malware kann auf verschiedene Weise in das Netzwerk eines Unternehmens eindringen. Um die Auswirkungen dieser schädlichen Software und Malware zu erkennen und zu mildern, können die AMP-Funktionen von FirePOWER verwendet werden, um die Übertragung von bösartiger Software und Malware im Netzwerk zu erkennen und optional zu blockieren.

Mithilfe der Dateikontrollfunktionen können Sie festlegen, ob Dateien hochgeladen und heruntergeladen werden sollen (erkennen), blockieren oder die Übertragung zulassen. Beispielsweise kann eine Dateirichtlinie implementiert werden, die das Herunterladen ausführbarer Dateien durch den Benutzer blockiert.

Mit der Network AMP-Funktionalität können Sie Dateitypen auswählen, die Sie über häufig verwendete Protokolle überwachen möchten, und SHA 256-Hashes, Metadaten aus den Dateien oder sogar Kopien der Dateien zur Malwareanalyse an die Cisco Security Intelligence Cloud senden. Die Cloud gibt basierend auf der Dateianalyse den Status von Datei-Hashes als unschädlich oder unschädlich zurück.

Dateikontrolle und AMP für FirePOWER können als Dateirichtlinie konfiguriert und als Teil Ihrer allgemeinen Zugriffssteuerungskonfiguration verwendet werden. Dateirichtlinien, die Zugriffskontrollregeln zugeordnet sind, überprüfen den Netzwerkverkehr, der die Regelbedingungen erfüllt.

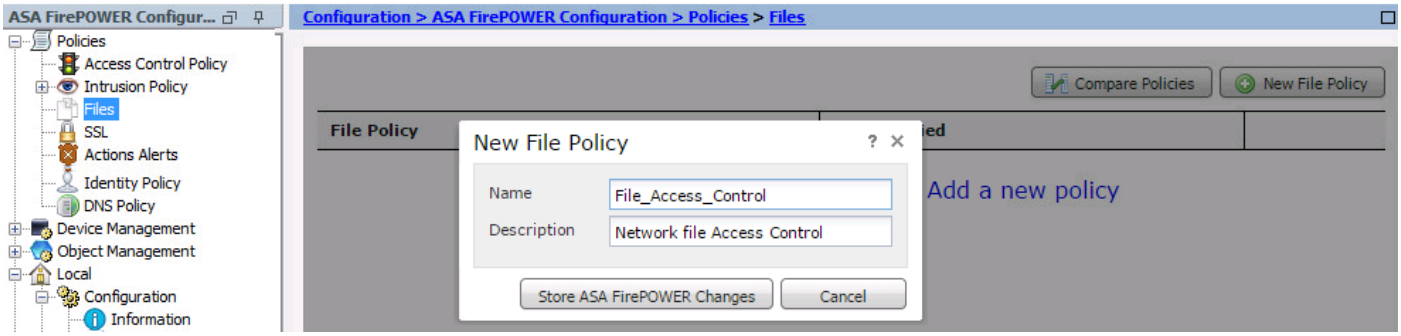
> **Hinweis**: Stellen Sie sicher, dass das FirePOWER-Modul über eine Protect/Control/Malware-Lizenz verfügt, um diese Funktion zu konfigurieren. Um die Lizenzen zu überprüfen, wählen Sie **Configuration > ASA FirePOWER Configuration > License.**

Konfigurieren der Dateirichtlinie für Dateikontrolle/Netzwerk-AMP

Dateizugriffskontrolle konfigurieren

Melden Sie sich bei ASDM an, und wählen Sie **Configuration > ASA FirePOWER Configuration > Policies > Files.** Das Dialogfeld **Neue Dateirichtlinie** wird angezeigt.

Geben Sie einen Namen und optional eine Beschreibung für Ihre neue Richtlinie ein, und klicken Sie dann auf **Store ASA FirePOWER Changes** Option. Die Seite Dateirichtlinien-Regel wird angezeigt.



Klicken Sie auf **Dateiregel hinzufügen**, um der Dateirichtlinie eine Regel hinzuzufügen. Die Dateiregel gibt Ihnen die präzise Kontrolle über Dateitypen, die Sie protokollieren, blockieren oder auf Malware prüfen möchten.

Anwendungsprotokoll: Geben Sie das Anwendungsprotokoll entweder als **Any** (Standard) oder als spezifisches Protokoll (HTTP, SMTP, IMAP, POP3, FTP, SMB) an.

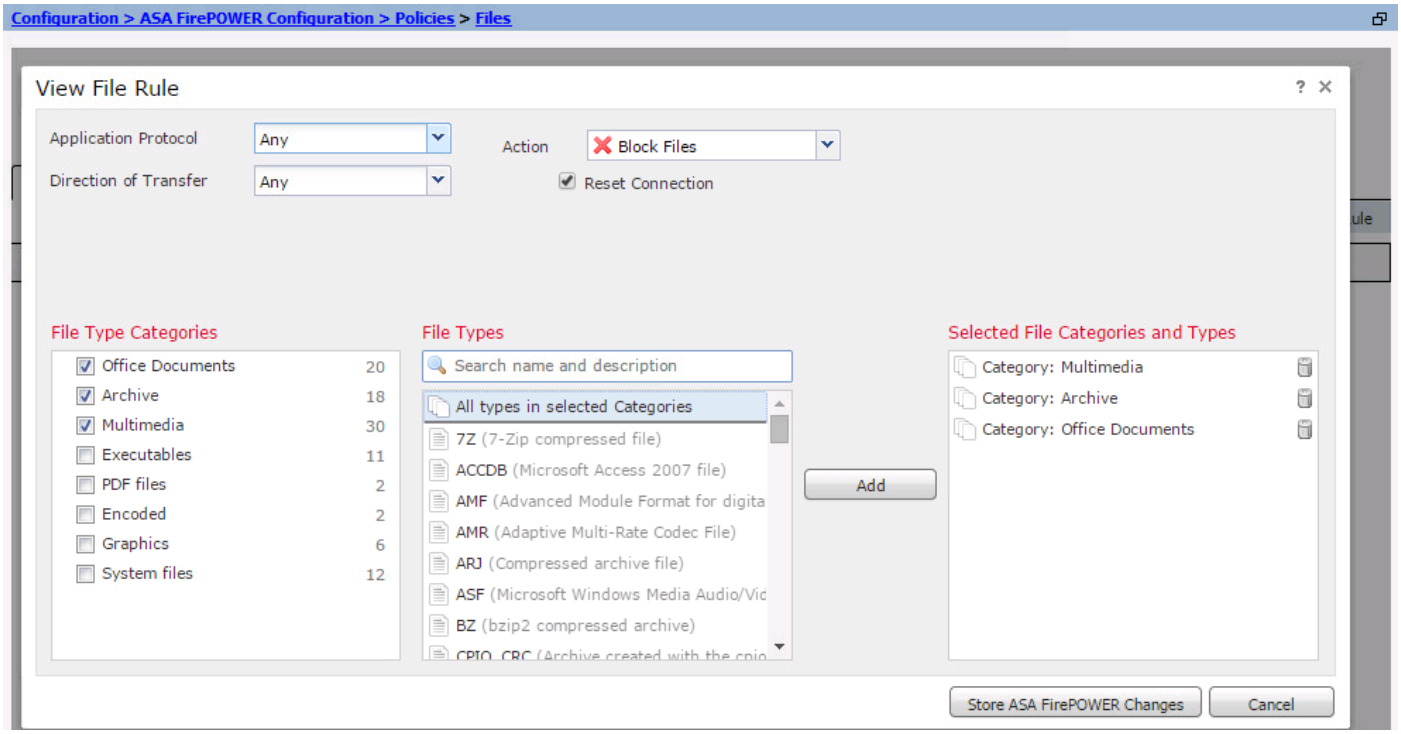
Übertragungsrichtung: Geben Sie die Richtung der Dateiübertragung an. Es kann entweder Any (Beliebig) oder Upload/Download (Hochladen/Herunterladen) basierend auf dem Anwendungsprotokoll sein. Sie können das Protokoll (HTTP, IMAP, POP3, FTP, SMB) für den Datei-Download und das Protokoll (HTTP, SMTP, FTP, SMB) für den Datei-Upload überprüfen. Verwenden Sie die **Any**-Option, um Dateien über mehrere Anwendungsprotokolle zu erkennen, unabhängig davon, ob Benutzer die Datei senden oder empfangen.

Aktion: Geben Sie die Aktion für die Dateizugriffskontrolle an. Die Aktion würde entweder **Dateien erkennen** oder **Dateien sperren. Detect File** action generiert das Ereignis und die **Blockdateien-**Aktion generiert das Ereignis und blockiert die Dateiübertragung. Bei der Aktion **Dateien sperren** können Sie optional **Verbindung zurücksetzen** auswählen, um die Verbindung zu beenden.

Dateityp-Kategorien: Wählen Sie die Dateityp-Kategorien aus, für die Sie die Datei blockieren oder die Warnmeldung generieren möchten.

Dateitypen: Wählen Sie Dateitypen aus. Die Option Dateitypen bietet eine detailliertere Option zur Auswahl des bestimmten Dateityps.

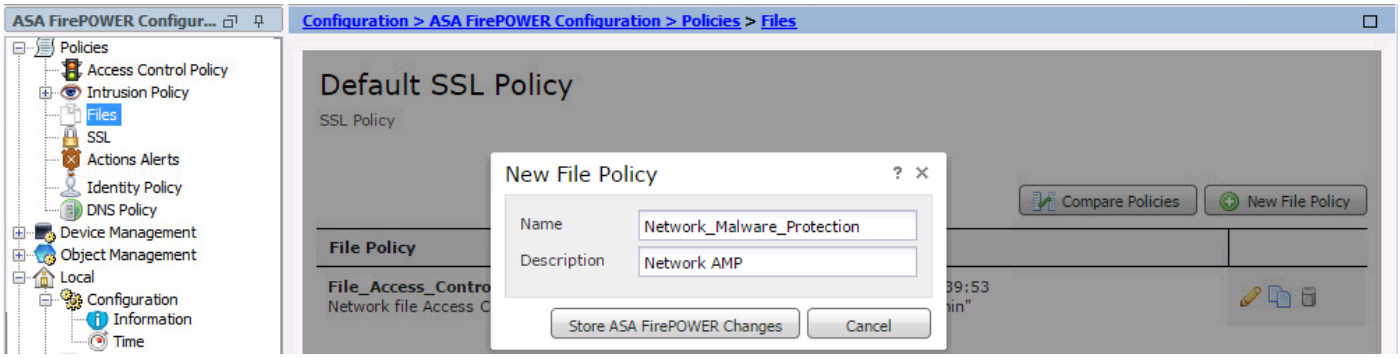
Wählen Sie die Option **Store ASA FirePOWER Changes** aus, um die Konfiguration zu speichern.



Netzwerk-Malware-Schutz (Netzwerk-AMP) konfigurieren

Melden Sie sich beim ASDM an, und navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Files.** Die Seite Dateirichtlinie wird angezeigt. Klicken Sie nun auf das Dialogfeld Neue Dateirichtlinie.

Geben Sie einen **Namen** und eine optionale **Beschreibung** für Ihre neue Richtlinie ein, und klicken Sie dann auf die Option **ASA Firepower Changes speichern**. Die Seite Dateirichtlinien wird angezeigt.



Klicken Sie auf die Option **Dateiregel hinzufügen**, um der Dateirichtlinie eine Regel hinzuzufügen. Dateiregel gibt Ihnen die präzise Kontrolle über Dateitypen, die Sie protokollieren, blockieren oder auf Malware prüfen möchten.

Anwendungsprotokoll: Geben Sie entweder Any (Standard) oder spezifisches Protokoll an (HTTP, SMTP, IMAP, POP3, FTP, SMB).

Übertragungsrichtung: Geben Sie die Richtung der Dateiübertragung an. Es kann entweder Any (Beliebig) oder Upload/Download (Hochladen/Herunterladen) basierend auf dem Anwendungsprotokoll sein. Sie können das Protokoll (HTTP, IMAP, POP3, FTP, SMB) auf Dateidownload und -protokoll (HTTP, SMTP, FTP, SMB) überprüfen, um Dateien hochzuladen. Verwenden Sie **Any**-Option, um Dateien über mehrere Anwendungsprotokolle zu erkennen, unabhängig davon, ob Benutzer die Datei senden oder empfangen.

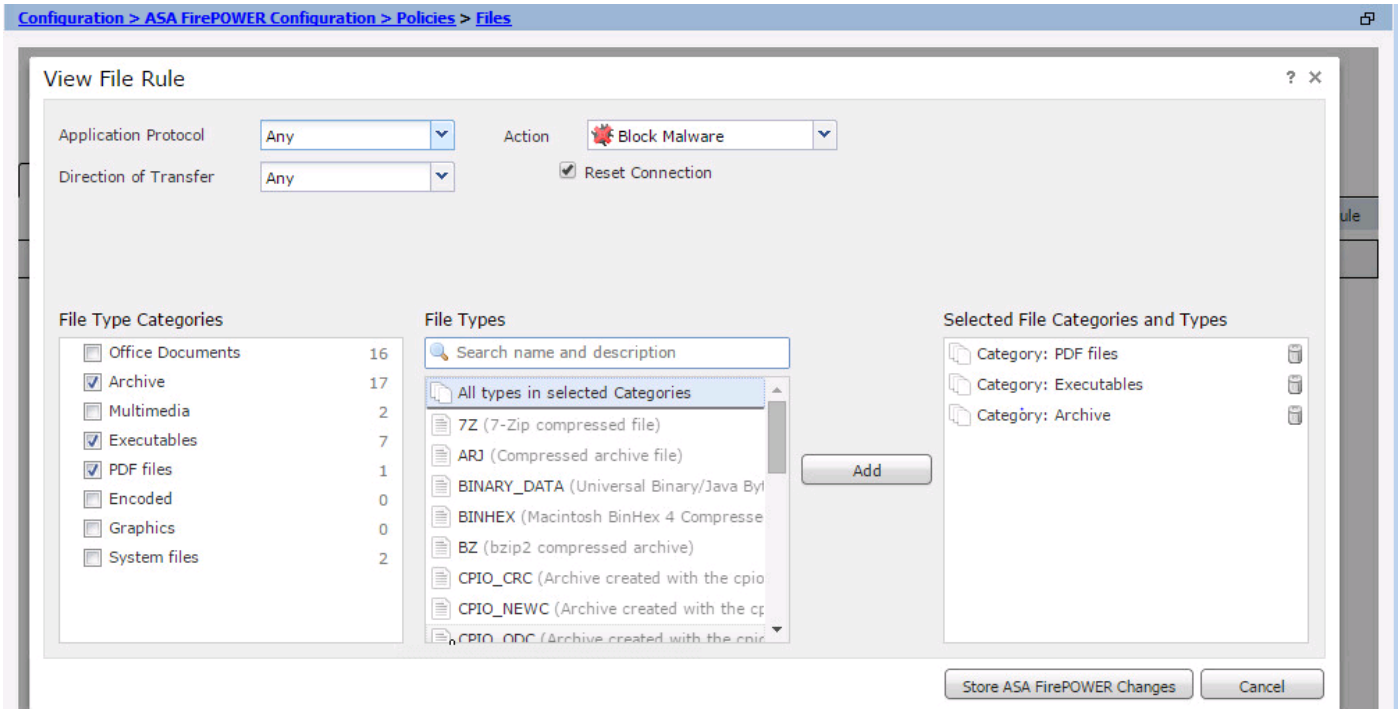
Aktion: Für die Funktion zum Schutz vor Malware im Netzwerk wäre die Aktion entweder **Malware Cloud Lookup** oder **Malware blockieren.** Action **Malware Cloud Lookup** generiert nur ein Ereignis, während Action **Block Malware** das Ereignis generiert und die Malware-Dateiübertragung blockiert.

> **Hinweis**: **Malware Cloud Lookup andBlock Malware** Rules ermöglichen es der FirePOWER, den SHA-256-Hash zu berechnen und zur Cloud-Suche zu senden, um festzustellen, ob Dateien, die das Netzwerk durchlaufen, Malware enthalten.

Dateityp-Kategorien: Wählen Sie die spezifischen Dateikategorien aus.

Dateitypen: Wählen Sie die spezifischen **Dateitypen** für detailliertere Dateitypen aus.

Wählen Sie Option **Store ASA FirePOWER Changes**, um die Konfiguration zu speichern.

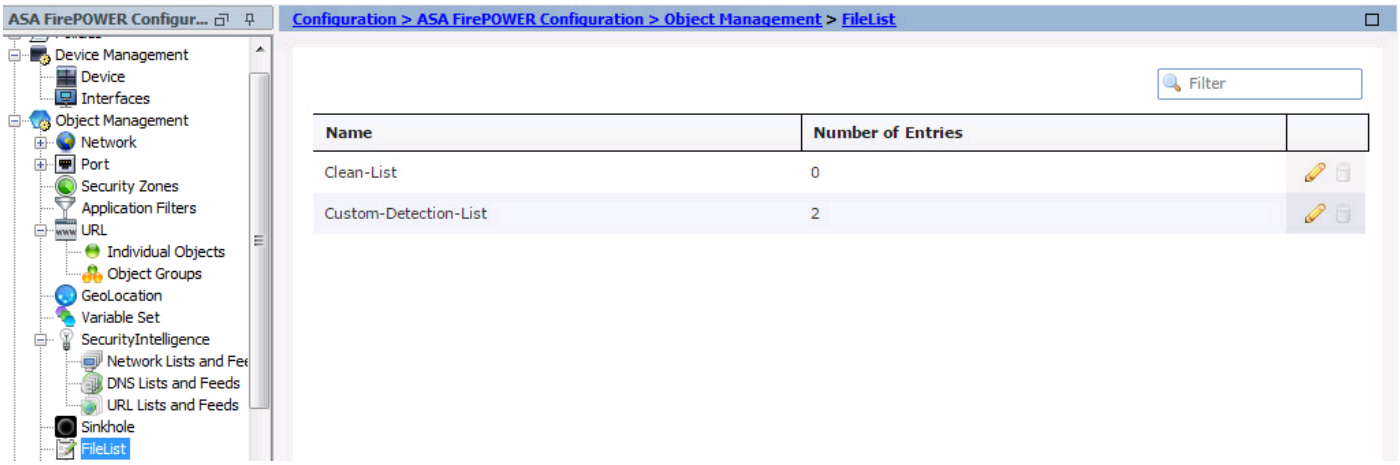


> **Hinweis**: Dateirichtlinien behandeln Dateien in der folgenden Reihenfolge von Regelaktionen: Die Blockierung hat Vorrang vor der Malware-Prüfung, die Vorrang vor der einfachen Erkennung und Protokollierung hat.

Wenn Sie einen netzwerkbasierten erweiterten Malware-Schutz (AMP) konfigurieren und die Cisco Cloud die Einstufung einer Datei falsch erkennt, können Sie die Datei der Dateiliste hinzufügen, indem Sie einen SHA-256-Hash-Wert verwenden, um die Einstufung der Datei in Zukunft zu verbessern. Je nach Dateityp haben Sie folgende Möglichkeiten:

- Um eine Datei so zu behandeln, als ob die Cloud eine saubere Einstufung zugewiesen hätte, fügen Sie die Datei der Liste "clean" hinzu.
- Um eine Datei so zu behandeln, als ob die Cloud eine Malware-Einstufung zugewiesen hätte, fügen Sie die Datei der benutzerdefinierten Liste hinzu.

Um dies zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > File List** und bearbeiten Sie die Liste, um SHA-256 hinzuzufügen.



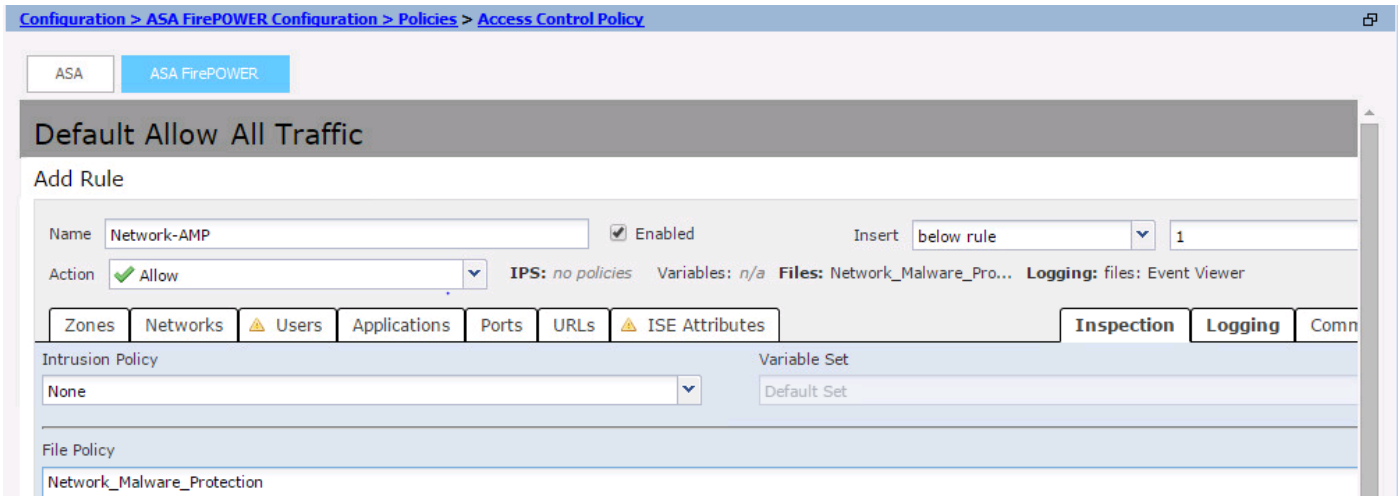
Konfigurieren der Zugriffskontrollrichtlinie für Dateirichtlinien

Navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy,** und erstellen Sie entweder eine neue **Zugriffsregel** oder bearbeiten Sie vorhandene **Zugriffsregeln,** wie in diesem Bild gezeigt.

Um die Dateirichtlinie zu konfigurieren, muss Aktion **zugelassen** sein. Navigieren Sie zur Registerkarte **Inspektion**, und wählen Sie die **Dateirichtlinie** aus dem Dropdown-Menü aus.

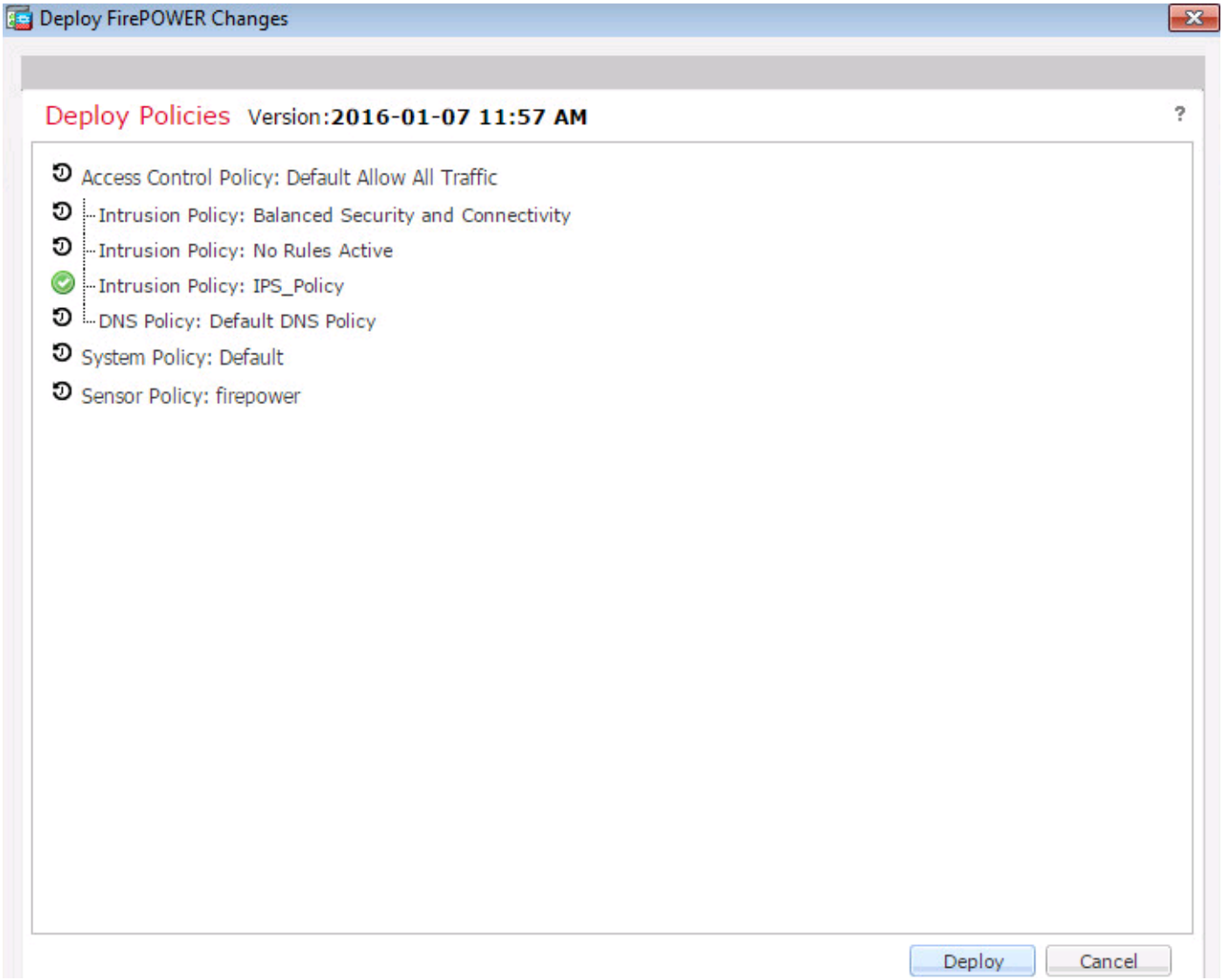
Um die Protokollierung zu aktivieren, navigieren Sie zur **Protokollierungsoption**, und wählen Sie die entsprechende Protokollierungsoption und die Option **Protokolldateien aus**. Klicken Sie auf die Schaltfläche **Speichern/Hinzufügen**, um die Konfiguration zu speichern.

Wählen Sie Option **Store ASA FirePOWER Changes** aus, um die AC-Richtlinienänderungen zu speichern.



Bereitstellung einer Zugriffskontrollrichtlinie

Navigieren Sie zur ASDMs **Deploy**-Option, und wählen Sie im Dropdown-Menü **die** Option **Firepower Change** bereitstellen. Klicken Sie auf die Option **Bereitstellen**, um die Änderungen bereitzustellen.

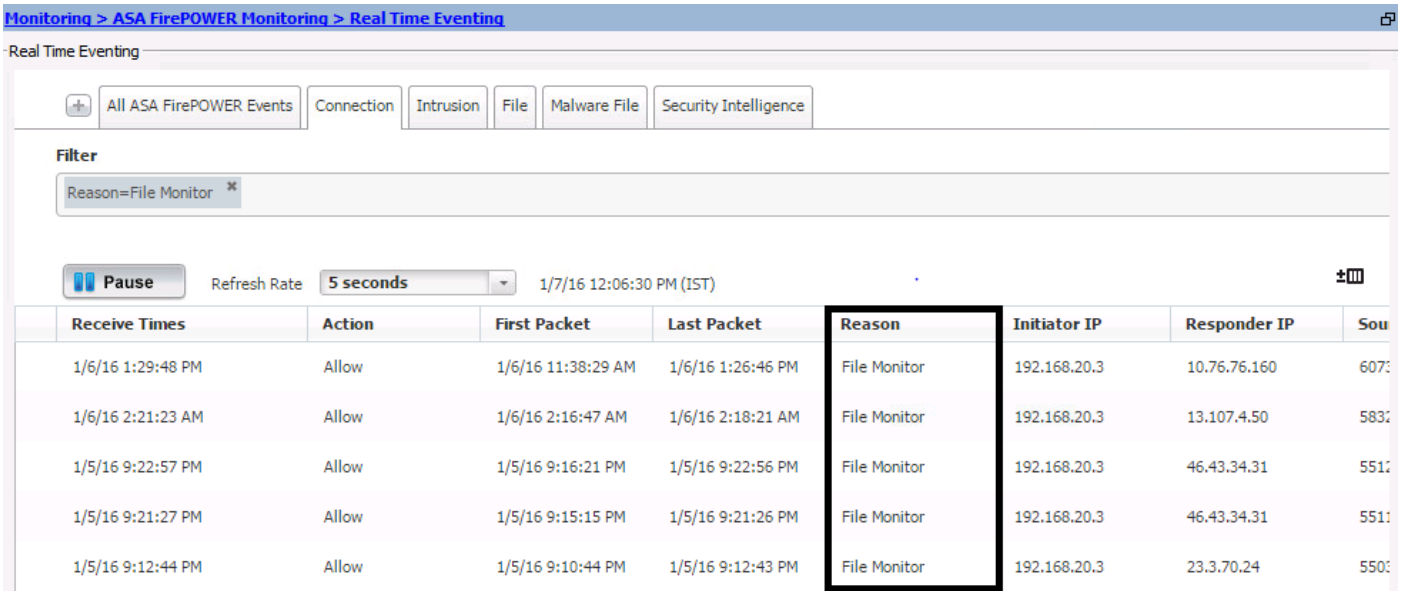


Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Task Status.** Stellen Sie sicher, dass die Aufgabe abgeschlossen sein muss, um die Konfigurationsänderung anzuwenden.

> **Hinweis**: In Version 5.4.x müssen Sie auf **ASA FirePOWER Changes** klicken, um die Zugriffsrichtlinie auf den Sensor anzuwenden.

Überwachung der Verbindung für Dateirichtlinienereignisse

Um die vom FirePOWER-Modul generierten Ereignisse im Zusammenhang mit Dateirichtlinien anzuzeigen, navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Real Time Event.**



Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Stellen Sie sicher, dass die Dateirichtlinie korrekt mit Protokoll/Richtung/Aktion/Dateitypen konfiguriert ist. Stellen Sie sicher, dass die richtige Dateirichtlinie in den Zugriffsregeln enthalten ist.

Stellen Sie sicher, dass die Bereitstellung der Zugriffskontrollrichtlinie erfolgreich abgeschlossen ist.

Überwachen Sie die Verbindungs- und Dateiereignisse (**Überwachung > ASA FirePOWER Monitoring > Real Time Eventing**), um zu überprüfen, ob der Datenverkehrsfluss die richtige Regel trifft oder nicht.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems