ASDM を使用してネットワーク AMP 用またはファイル制御用に FirePOWER モジュールを設定する。

目次

概要

このドキュメントでは、ネットワークの高度なマルウェア防御（AMP）や FirePOWER モジュールのファイル アクセス コントロール機能、および Adaptive Security Device Manager（ASDM）でのこれらの設定方法について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- 適応型セキュリティ アプライアンス（ASA）ファイアウォールと ASDM の知識。
- FirePOWER アプライアンスの知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 5.4.1 以降が稼働する ASA Firepower モジュール（ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X）。
- ソフトウェア バージョン 6.0.0 以降が稼働する ASA Firepower モジュール（ASA 5515-X、

ASA 5525-X、ASA 5545-X、ASA 5555-X）。
- ASDM 7.5.1 以降。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

悪意のあるソフトウェア/マルウェアは、組織のネットワークに複数の方法で侵入する可能性があります。 この悪意のあるソフトウェアとマルウェアの影響を特定し、軽減するために、FirePOWER の AMP 機能を使い、ネットワーク上の悪意のあるソフトウェアとマルウェアの伝送を検出し、必要に応じてブロックすることができます。

ファイル制御機能を使い、ファイル アップロードおよびダウンロードの転送をモニタ（検出）、ブロックまたは許可することを選択できます。 たとえば、ユーザが実行可能なファイルのダウンロードをブロックするためのファイル ポリシーを実装できます。

ネットワーク AMP 機能を使うと、一般的に使用されるプロトコルでモニタしたいファイル タイプを選択でき、SHA 256 ハッシュやファイルからのメタデータを送信できます。またはマルウェア分析のため、ファイル自体を Cisco セキュリティ インテリジェンス クラウドにコピーすることもできます。 クラウドは、ファイル分析に基づき、ファイル ハッシュの性質がクリーンか悪意があるものかを返します。

Firepower のファイル コントロールと AMP はファイル ポリシーとして設定でき、全体的なアクセス コントロール設定の一部として使用できます。 アクセス コントロール ルールに関連付けられたファイル ポリシーは、ルール条件を満たすネットワーク トラフィックを検査します。

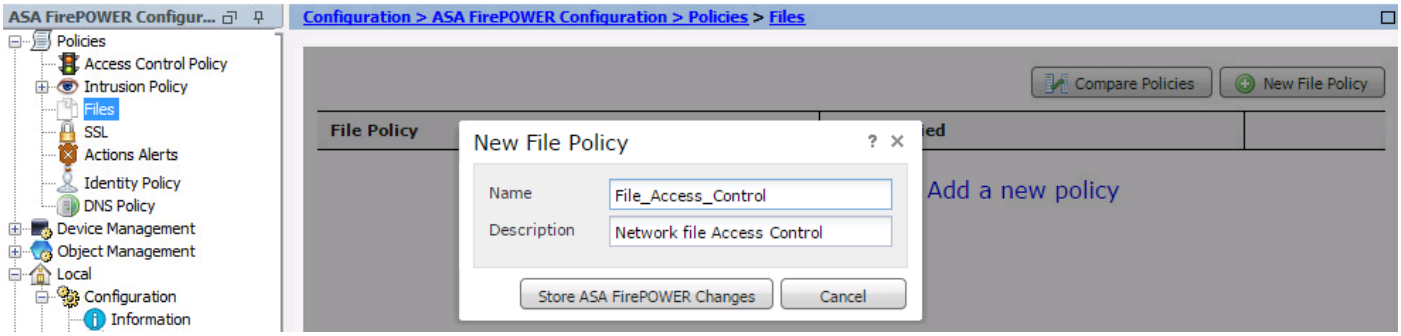
> **注:** この機能を設定するためには、FirePOWER モジュールが保護/制御/マルウェアのライセンスを取得していることを確認します。 ライセンスを確認するには、[Configuration] > [ASA FirePOWER Configuration] > [License] を選択します。

ファイル制御/ネットワーク AMP のファイル ポリシーの設定

ファイル アクセス コントロールの設定

ASDM にログインし、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Files] を選択します。 [New File Policy] ダイアログ ボックスが表示されます。

新しいポリシーの [Name] と [Description] を入力し、[Store ASA Firepower Changes] オプションをクリックします。 [File Policy Rule] ページが表示されます。



ルールをファイル ポリシーに追加するには、[Add File Rule] をクリックします。 ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。

Application Protocol： [application protocol] には [Any]（デフォルト）または特定のプロトコル（HTTP、SMTP、IMAP、POP3、FTP、SMB）を指定します。

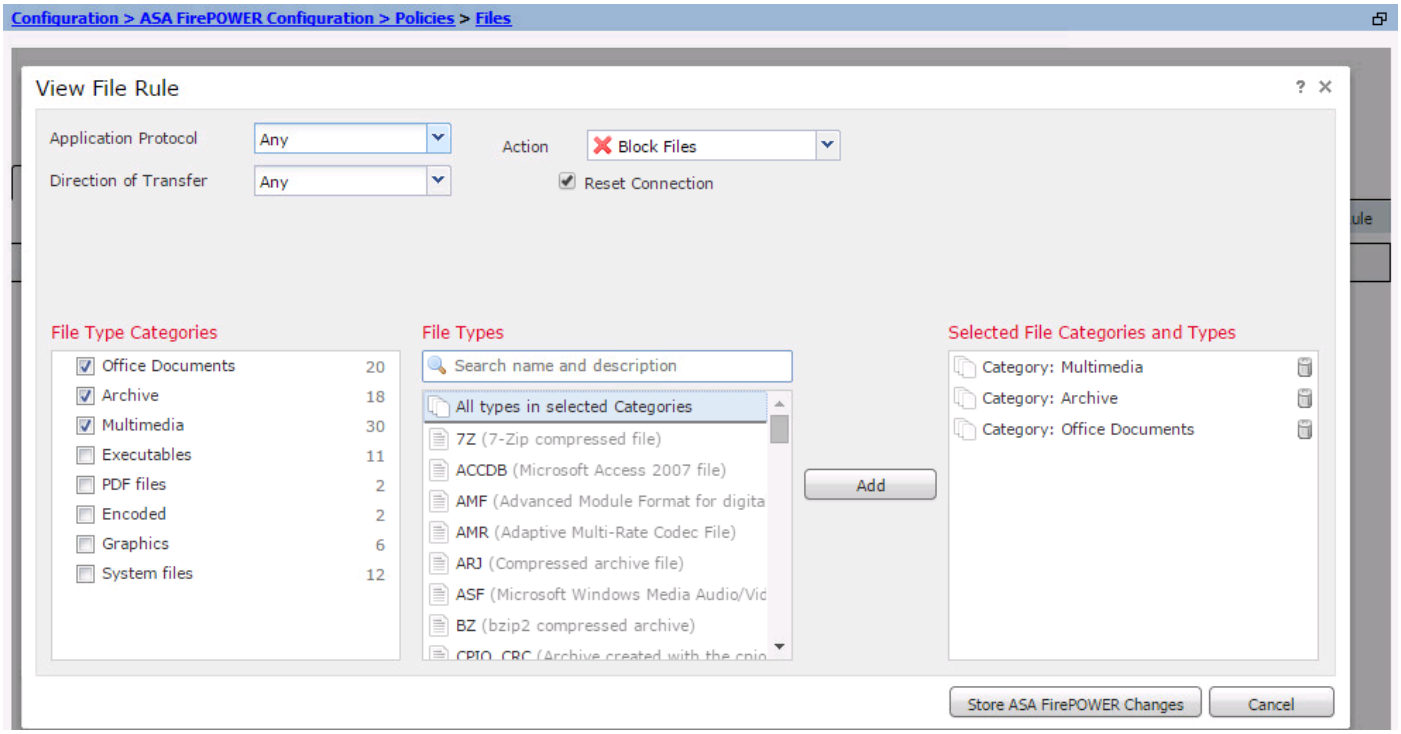
Direction of Transfer： ファイル転送の方向を指定します。 これは [Application protocol] に基づき、[Any] または [Upload/Download] のどちらかになります。 ファイルのダウンロードの場合、プロトコル（HTTP、IMAP、POP3、FTP、SMB）を、ファイルのアップロードの場合、プロトコル（HTTP、SMTP、FTP、SMB）を検査できます。 ユーザがファイルを送信または受信したかに関わらず、複数のアプリケーション プロトコルでファイルを検出するには、[Any] オプションを使用します。

アクション： ファイル アクセス コントロール機能の動作を指定します。 [Action] は [Detect Files] または [Block Files] のどちらかです。 [Detect Files] アクションはイベントを生成し、[Block Files] アクションはイベントを生成し、ファイル転送をブロックします。 [Block Files] アクションでは、必要に応じて、接続を終了する [Reset Connection] を選択できます。

File Type Categories： ブロックするかアラートを生成したいファイル タイプのカテゴリを選択します。

File Types： ファイル タイプを選択します。 [File Types] オプションは、特定のファイル タイプを選択できる、より詳細なオプションです。

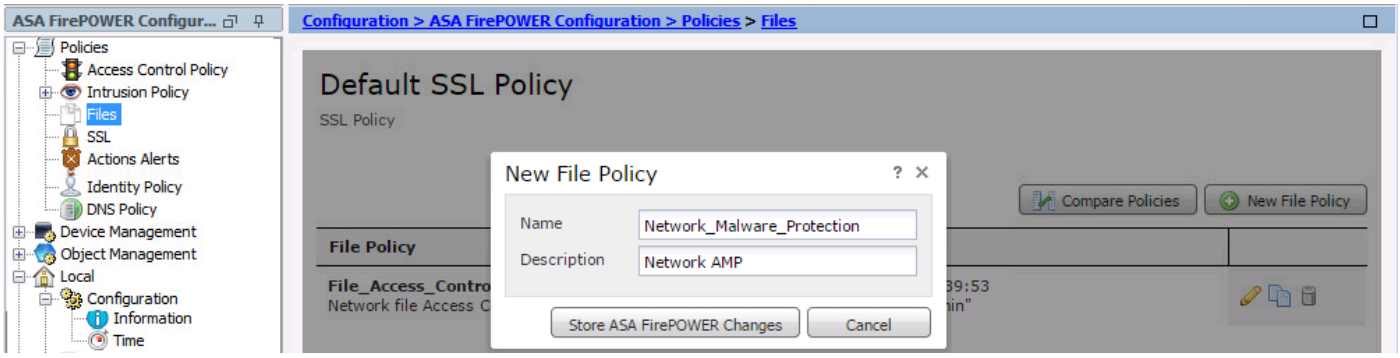
[Store ASA Firepower Changes] オプションを選択し、設定を保存します。



ネットワーク マルウェア防御（ネットワーク AMP）の設定

ASDM にログインし、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Files] に移動します。 [File Policy] ページが表示されます。 ここで、表示された [New File Policy] ダイアログボックスをクリックします。

新しいポリシーの [Name] と [Description]（任意）を入力し、[Store ASA Firepower Changes] オプションをクリックします。 [File Policy Rules] ページが表示されます。



ファイル ポリシーにルールを追加するには、[Add File Rule] オプションをクリックします。 ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。

Application Protocol： [Any]（デフォルト）または特定のプロトコル（HTTP、SMTP、IMAP、POP3、FTP、SMB）を指定します。

Direction of Transfer： ファイル転送の方向を指定します。 これは [Application protocol] に基づき、[Any] または [Upload/Download] のどちらかになります。 ファイルのダウンロードの場合、プロトコル（HTTP、IMAP、POP3、FTP、SMB）を、ファイルのアップロードの場合、プロトコル（HTTP、SMTP、FTP、SMB）を検査できます。 ユーザがファイルを送信または受信したかに関わらず、複数のアプリケーション プロトコルでファイルを検出するには、[Any] オプションを使用します。

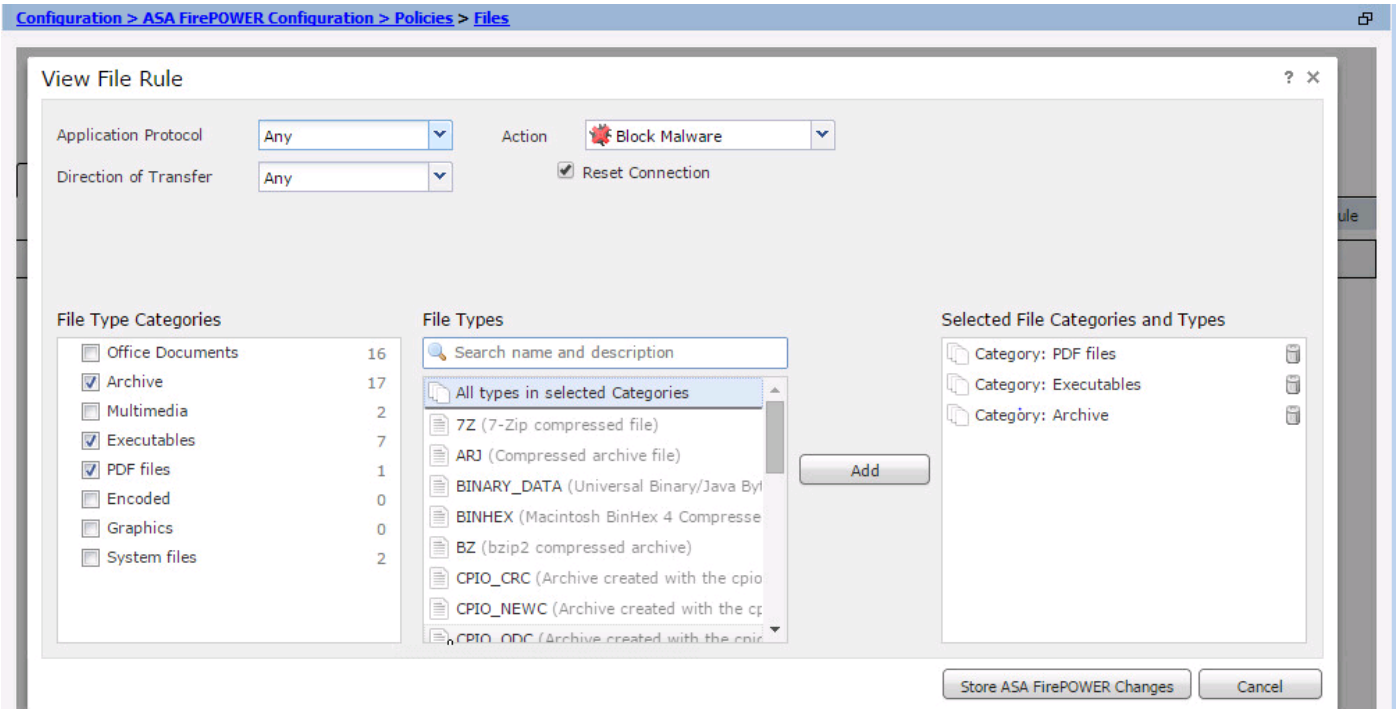
アクション： ネットワーク マルウェア防御機能では、[Action] は [Malware Cloud Lookup] または [Block Malware] のいずれかです。 [Action] が [Malware Cloud Lookup] の場合、イベントを生成するだけであるのに対し、[Block Malware] はイベントを生成するだけでなく、マルウェア ファイルの転送をブロックします。

> **注:** [Malware Cloud Lookup] および [Block Malware] ルールにより、Firepower が SHA-256 ハッシュを計算し、クラウド ルックアップ プロセスにそれを送信し、ネットワーク上を伝送されるファイルにマルウェアが含まれているかどうかを判断します。

File Type Categories： 特定のファイル カテゴリを選択します。

File Types： より詳細なファイル タイプとして、特定の [File Types] を選択します。

[Store ASA Firepower Changes] オプションを選択し、設定を保存します。

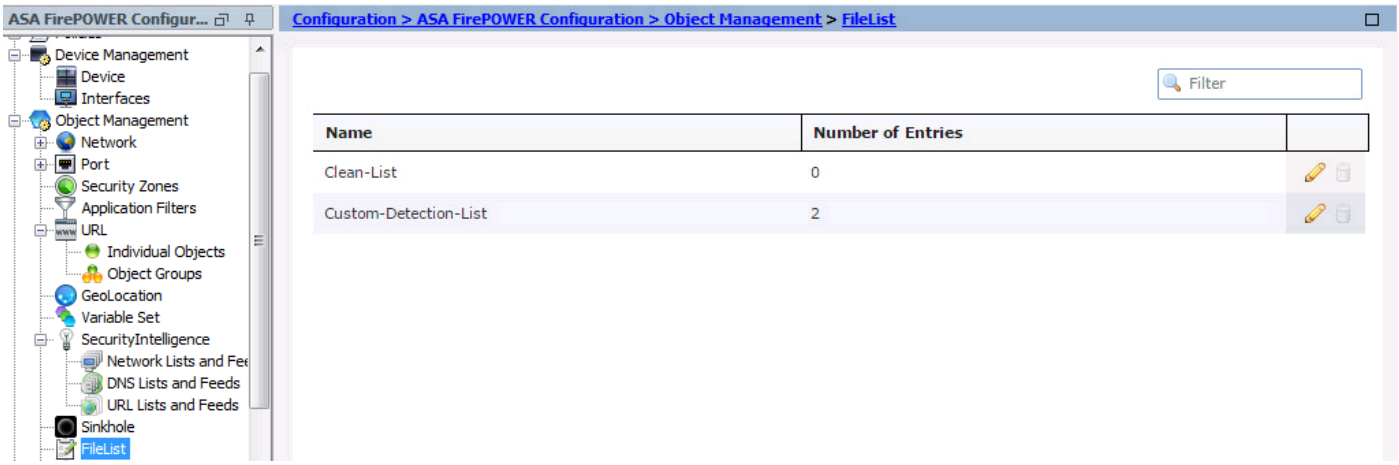


> **注:** ファイル ポリシーは次のルール-アクションの順でファイルを処理します。（優先度の高い順に）ブロッキング、次にマルウェア インスペクション、さらにその次に単純な検出とロギングとなります。

ネットワークベースの高度なマルウェア防御（AMP）を設定し、Cisco クラウドがファイルの性質を誤って検出した場合、SHA-256 ハッシュ値を使ってそのファイルをファイル リストに追加すると、その後、ファイルの性質がより適切に検出されるようになります。 ファイル リストのタイプに応じて、次の操作を実行できます。

- クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム リストにファイルを追加します。

これを設定するには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [File List] に移動し、SHA-256 を追加するよう、リストを編集します。



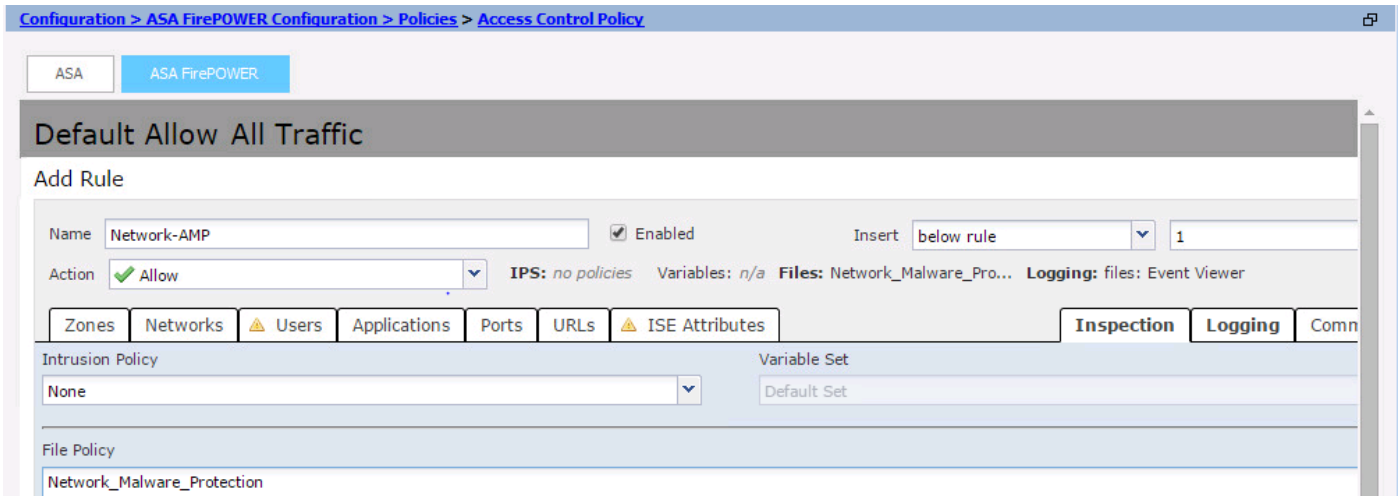
ファイル ポリシーのアクセス コントロール ポリシーの設定

[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control Policy] に移動し、次に示すように、新しい [Access Rule] を作成するか、既存の [Access Rule] を編集します。

ファイル ポリシーを設定するには、[Action] は [Allow] にする必要があります。 [Inspections] タブに移動し、ドロップ ダウン メニューから [File Policy] を選択します。

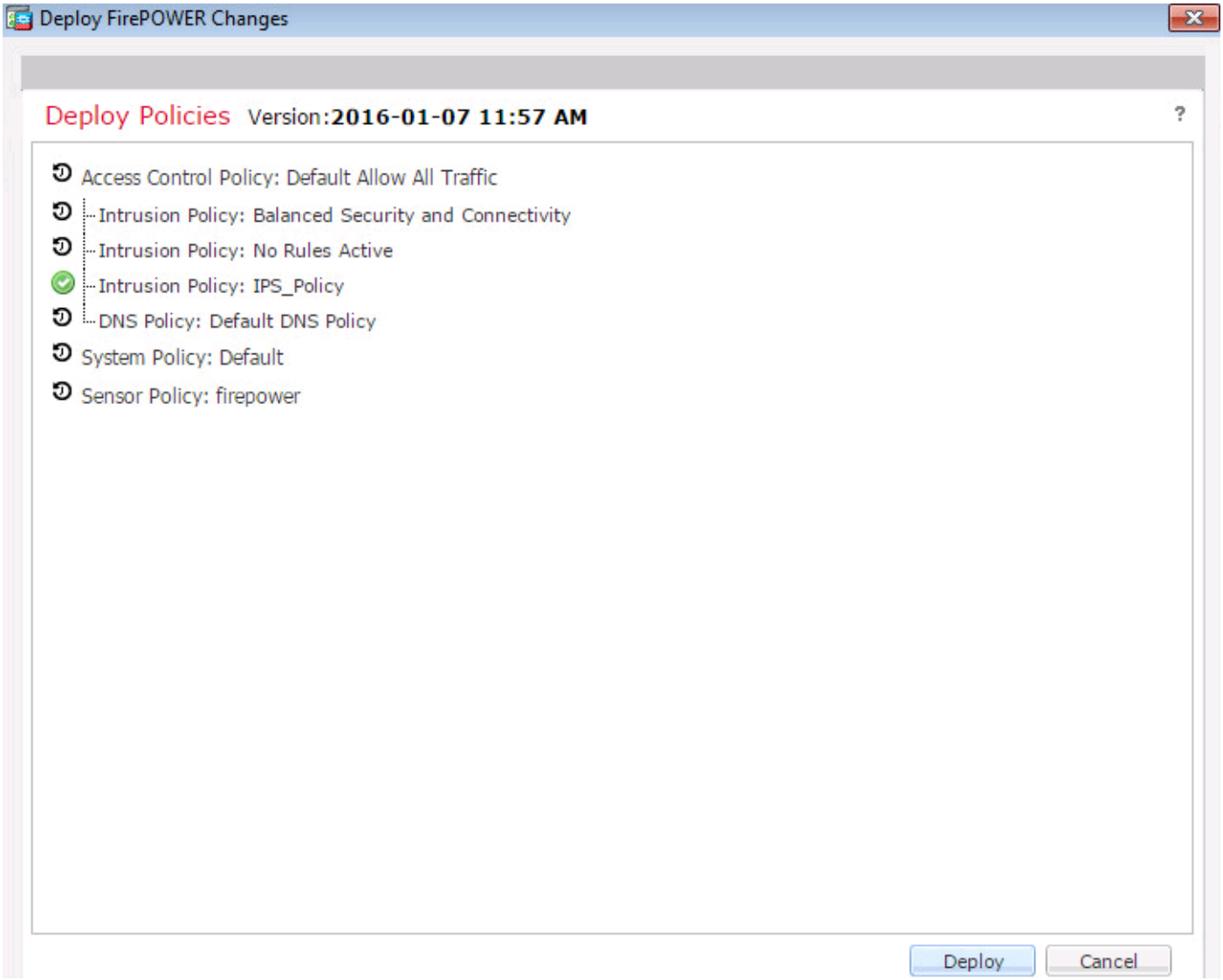
ロギングを有効にするには、[logging] オプションに移動し、適切な [logging] オプションと [Log Files] オプションを選択します。 [Save/Add] ボタンをクリックして変更を保存します。

AC ポリシーの変更を保存するには、[Store ASA Firepower Changes] オプションを選択します。



アクセス コントロール ポリシーの展開

ASDM の [Deploy] オプションに移動し、ドロップ ダウン メニューから [Deploy Firepower Change] オプションを選択します。 変更を展開するには、[Deploy] オプションをクリックします。

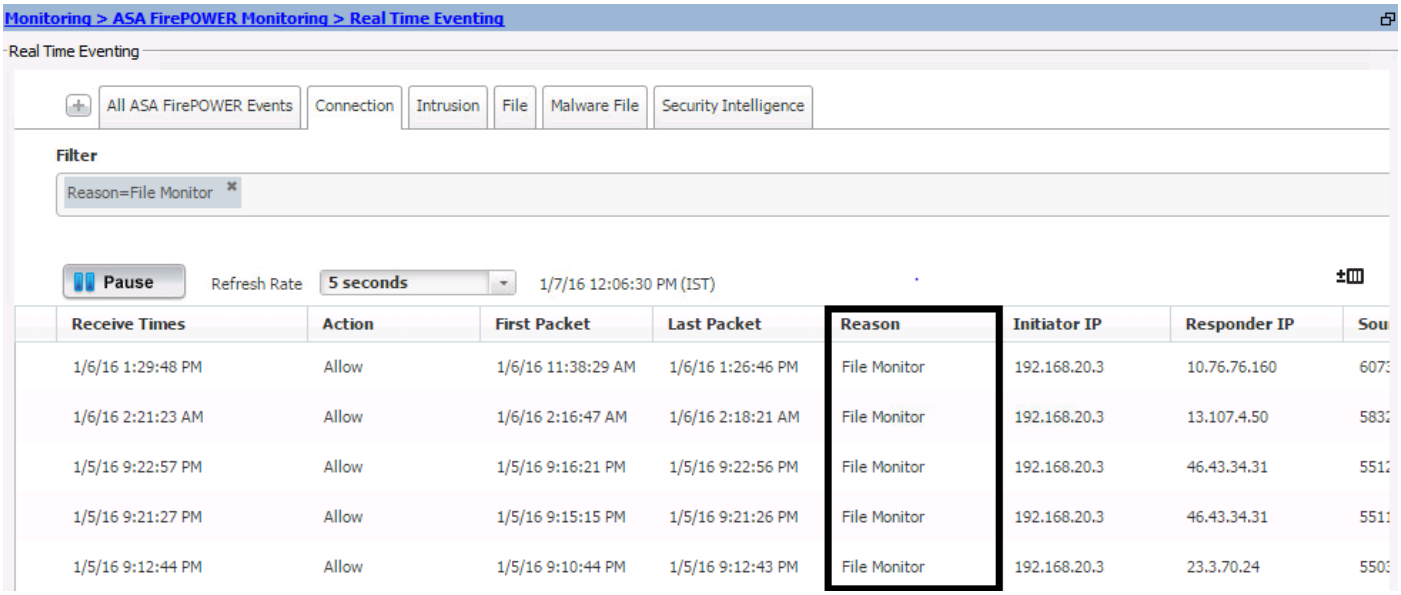


[Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動します。 設定変更を適用するためには、タスクを完了する必要があります。

> **注:** バージョン 5.4.x では、アクセス ポリシーをセンサーに適用するには、[ASA FirePOWER Changes] をクリックする必要があります。

ファイル ポリシー イベントのモニタ接続

ポリシーに関連した Firepower モジュールにより生成されたイベントを確認するには、[Monitoring] > [ASA Firepower Monitoring] > [Real Time Eventing] に移動します。



確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ファイル ポリシーが、プロトコル/方向/ アクション/ ファイル タイプについて正しく設定されていることを確認します。 正しいファイル ポリシーがアクセス ルールに含まれていることを確認します。

アクセス コントロール ポリシーの展開が正常に完了したことを確認します。

トラフィック フローが適切なルールに当たっているかどうかを確認するため、接続イベントとファイル イベントをモニタします（ [Monitoring] > [ASA Firepower Monitoring] > [Real Time Eventing] ）。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems