ASDM（On-BoxManagement）による Cisco セキュリティ インテリジェンスを使用する間の IP ブラックリストの設定

内容

概要

このドキュメントでは、Cisco Security Intelligence および IP アドレス レピュテーションの概要と、レピュテーションが低い IP アドレスのカスタム/自動フィードを使用しながら IP ブラックリスト（ブロッキング リスト）を構成する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あることが推奨されます。

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

Security Intelligence

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いています。

- 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）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

Cisco Security Intelligence は、Cisco TALOS チームによってレピュテーションが低いと判断された IP アドレスのコレクションからなります。これらのコレクションは、定期的に更新されます。.Cisco TALOS チームは、スパム、マルウェア、フィッシング攻撃などの不正なアクティビティの発信元 IP アドレスを、レピュテーションの低い IP アドレスとして判断します。

Cisco IP Security Intelligence フィードは、攻撃者のデータベース、Bogon、ボット、CnC、Dga、ExploitKit、マルウェア、Open_proxy、Open_relay、フィッシング、レスポンス、スパム、不審な IP アドレスを追跡します。FirePOWER モジュールには、レピュテーションの低い IP アドレスのカスタム フィードを作成するオプションがあります。

Security Intelligence フィードの概要

Security Intelligence で各種のカテゴリとして分類できる IP アドレス コレクションのタイプについて説明します。

攻撃者：継続的に脆弱性をスキャンしている IP アドレスや、他のシステムを悪用しようとする IP アドレスのコレクション。

マルウェア：マルウェアの伝播を試みている IP アドレスや、アクセスしてきた閲覧者をアクティブに攻撃する IP アドレスのコレクション。

フィッシング：アクティブにエンドユーザをだまして機密情報（ユーザ名やパスワード）を入力させようとするホストのコレクション

スパム：迷惑メールの送信元として識別されたホストのコレクション。

ボット：ボットネットの一部としてアクティブに参加しているホストや、既知のボットネット コントローラによって制御されているホストのコレクション。

CnC：既知のボットネットを制御しているサーバとして識別されたホストのコレクション。

OpenProxy：オープン Web プロキシを実行し、匿名 Web ブラウジング サービスを提供していることが判明したホストのコレクション。

OpenRelay：スパムやフィッシングの攻撃者が使用する匿名メール中継サービスを提供していることが判明したホストのコレクション。

TorExitNode：Tor アノニマイザー ネットワークの出口ノード サービスを提供していることが判

明したホストのコレクション。

Bogon：割り振られていないのにトラフィックを送信している IP アドレスのコレクション。

不審：不審なアクティビティを見せていているため、現在調査中の IP アドレスのコレクション。

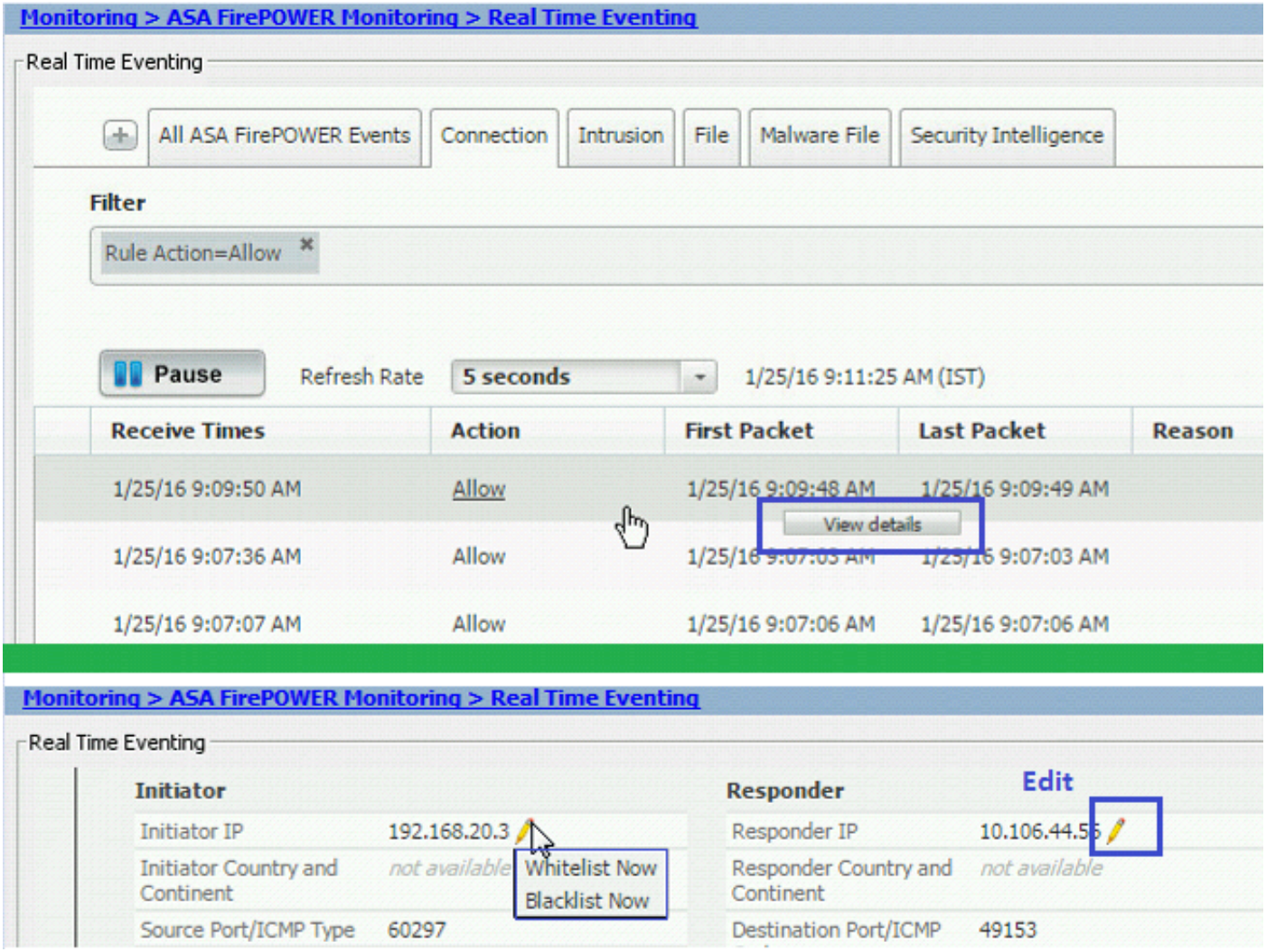
レスポンス：不審または不正な動作に関与していることが度々確認された IP アドレスのコレクション。

グローバル ブラックリストとグローバル ホワイトリストへの手動による IP アドレスの追加

特定の IP アドレスが不正なアクティビティに関与していることがわかった場合、FirePOWER モジュールを使用することで、その IP アドレスをグローバル ブラックリストに追加できます。ブラックリスト IP アドレスでブロックされている特定の IP アドレスに対してトラフィックを許可する必要がある場合は、その IP アドレスをグローバル ホワイトリストに追加することもできます。IP アドレスをグローバル ブラックリスト/グローバル ホワイトリストに追加すると、その変更は即時に適用されるため、ポリシーを適用する必要はありません。

IP アドレスをグローバル ブラックリスト/グローバル ホワイトリストに追加するには、[Monitoring] > [ASA FirePOWER Monitoring] > [Real Time Eventing] に移動し、マウスのカーソルを該当する接続イベントに合わせて [View Details] を選択します。

グローバル ブラックリスト/グローバル ホワイトリストには、送信元 IP アドレスまたは宛先 IP アドレスのいずれかを追加できます。[Edit] ボタンをクリックし、[Whitelist Now/Blacklist Now] を選択すると、該当するリストに IP アドレスが追加されます（次の図を参照）。



送信元または宛先 IP アドレスがグローバル ホワイトリスト グローバル ブラックリストに追加されたことを確認するには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、グローバル ブラックリスト/グローバル ホワイトリストを編集します。.また、削除ボタンを使用して、リストから IP アドレスを削除することもできます。

ブラックリスト IP アドレスのカスタム リストの作成

FirePOWER では、カスタム ネットワーク/IP アドレス リストを作成して、そのリストをブラックリスト（ブロッキング リスト）で使用できるようになっています。 それには次の方法があります。

1. IP アドレスをテキスト ファイルに書き込み（1 行につき 1 つの IP アドレス）、そのファイルを FirePOWER モジュールにアップロードします。**ファイルをアップロードするには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、[Add Network Lists and Feeds] をクリックします。** **[Name]：** カスタム リストの名前を指定します。 **Type:** ドロップダウン リストから [List] を選択します。 **[Upload List]：** [Browse] を選択して、システム内でアップロードするテキスト ファイルを見つけます。[Upload] オプションを選択してファイルをアップロードします。
2. サードパーティの IP データベースをカスタム リストとして使用することもできます。この場合、FirePOWER モジュールはサードパーティのサーバに接続して IP アドレス リストを取得します。このように設定するには、[Configuration] > [ASA FirePOWER Configuration] >

[Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、[Add Network Lists and Feeds] をクリックします。

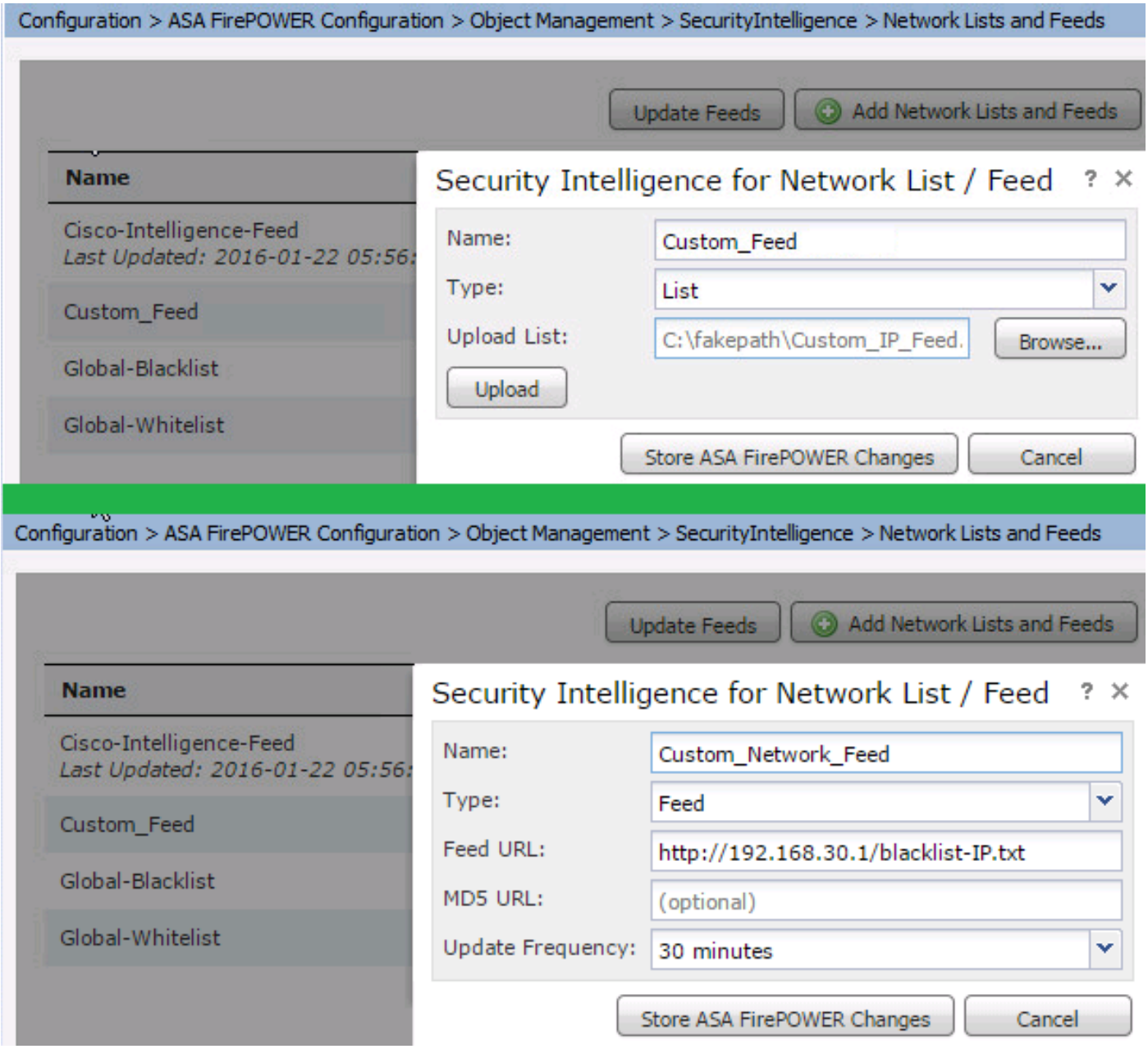
[Name]：カスタム フィードの名前を指定します。

Type:ドロップダウン リストから [Feed] オプションを選択します。

[Feed URL]：FirePOWER モジュールが接続してフィードをダウンロードするために使用するサーバの URL を指定します。

[MD5 URL]：フィードの URL パスを検証するために使用するハッシュ値を指定します。

[Update Frequency]：システムが URL フィード サーバに接続する時間間隔を指定します。



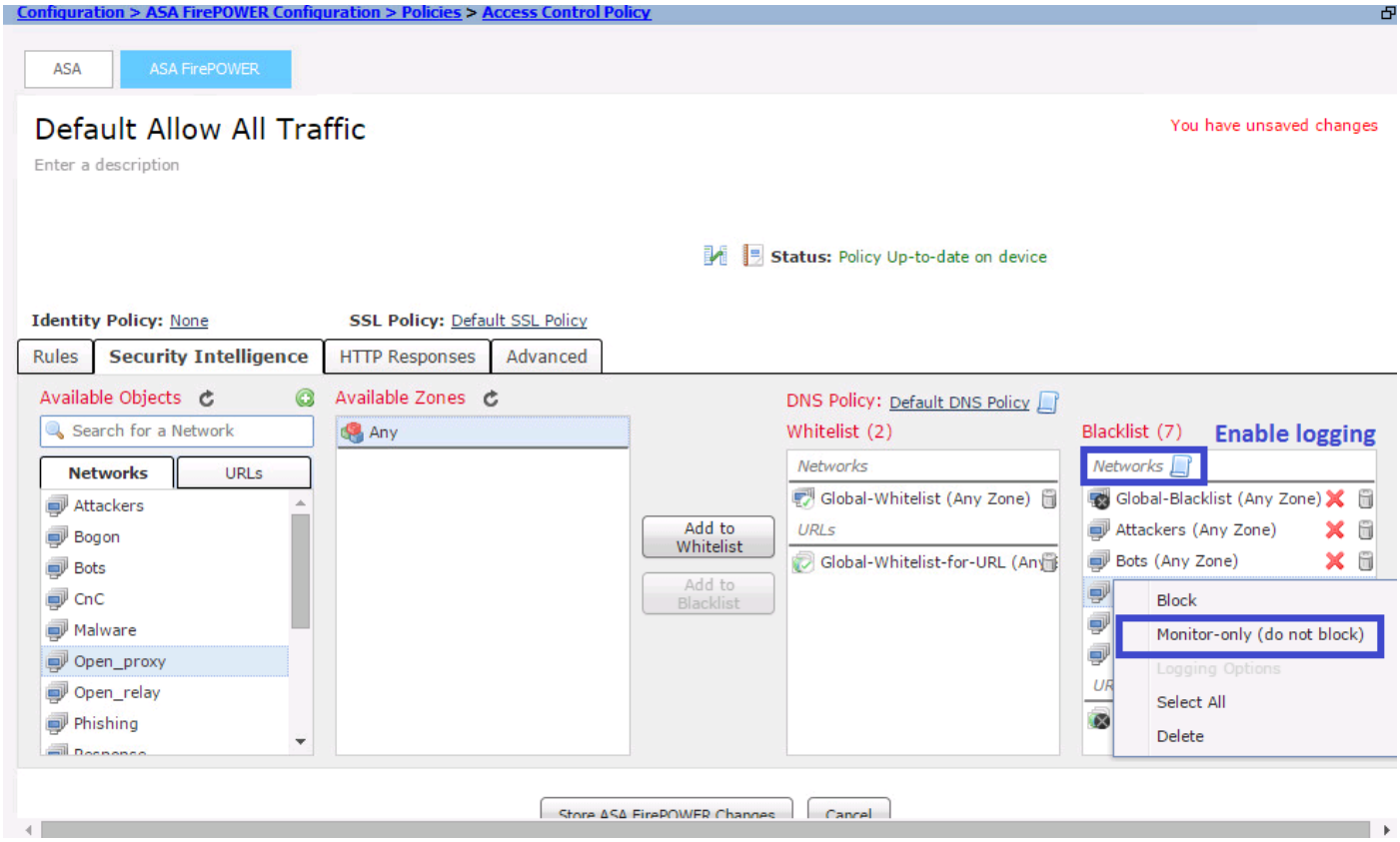
Security Intelligence の設定

Security Intelligence を設定するには、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control Policy] に移動して、[Security Intelligence] タブを選択します。

[Available Object] の [Networks] から目的のフィードを選択し、[Whitelist/Blacklist] 列に移動して、不正な IP アドレスに対する接続を許可/ブロックします。

次の図に示されているアイコンをクリックすると、ロギングを有効にすることができます。

不正な IP 接続をブロックするのではなく、不正な IP 接続に対してイベントが生成されるだけにするには、フィードを右クリックして [Monitor-only (do not block)] を選択します (図を参照) 。

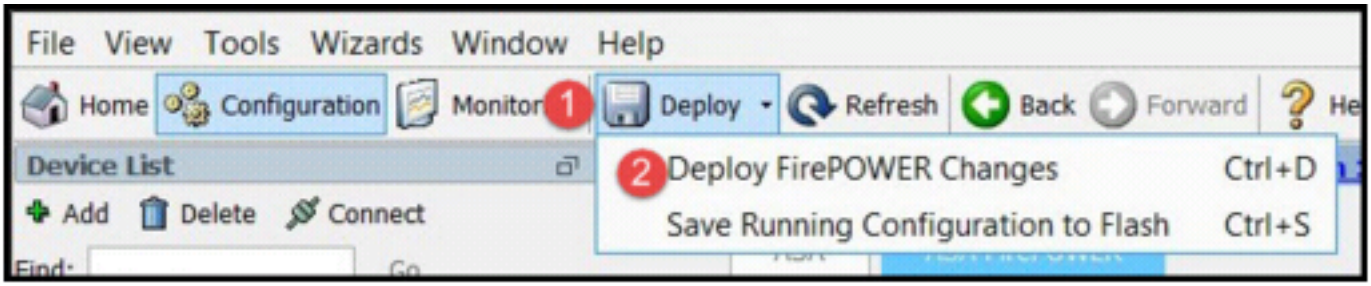


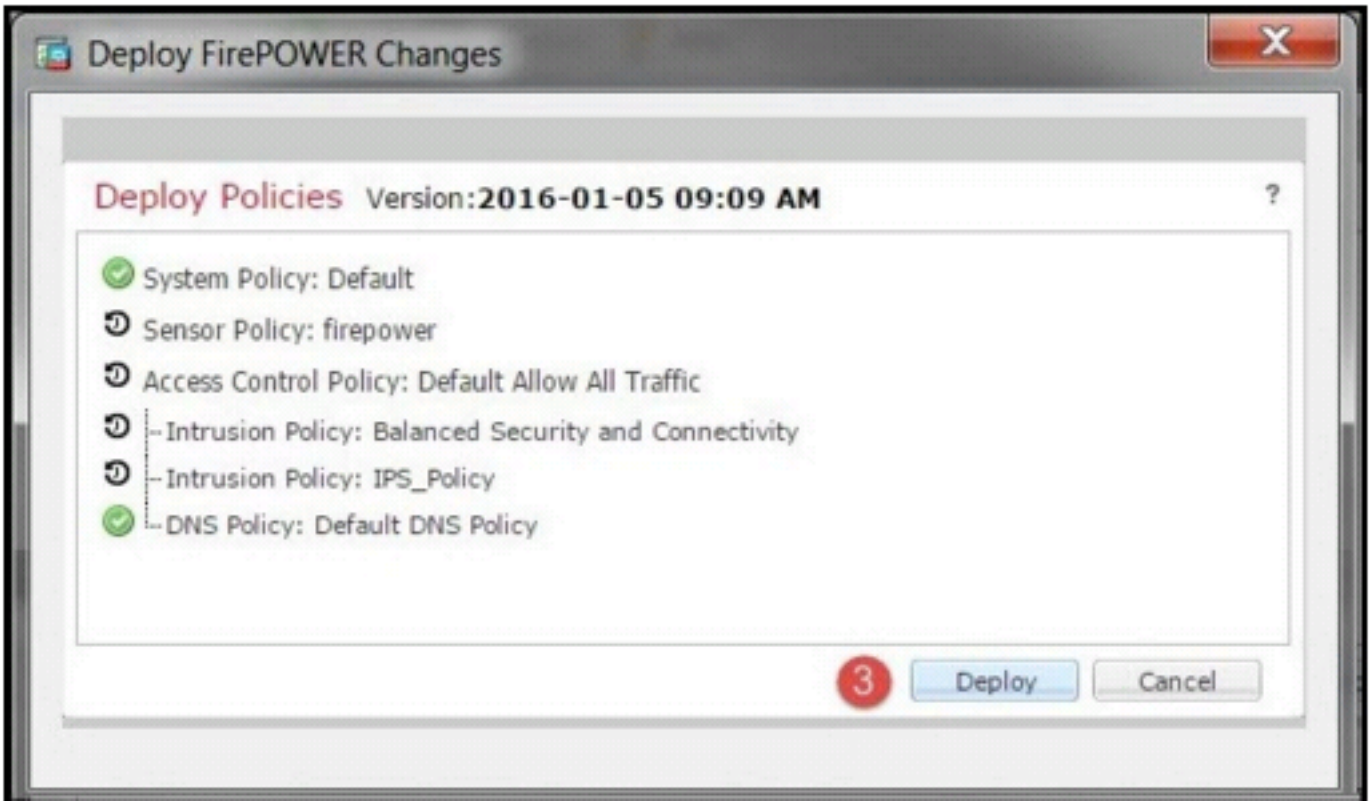
AC ポリシーの変更を保存するには、[Store ASA Firepower Changes] オプションを選択します。

アクセス コントロール ポリシーの展開

変更を適用するには、アクセス コントロール ポリシーを導入する必要があります。ポリシーを適用する前に、デバイス上のアクセス コントロール ポリシーが古いものであるかを示す標識を確認してください。

センサーに変更を導入するには、c[Deploy] をクリックし、[**Deploy FirePOWER Changes**]を選択し、ポップアップウィンドウで[**Deploy**]を選択して変更を導入します。



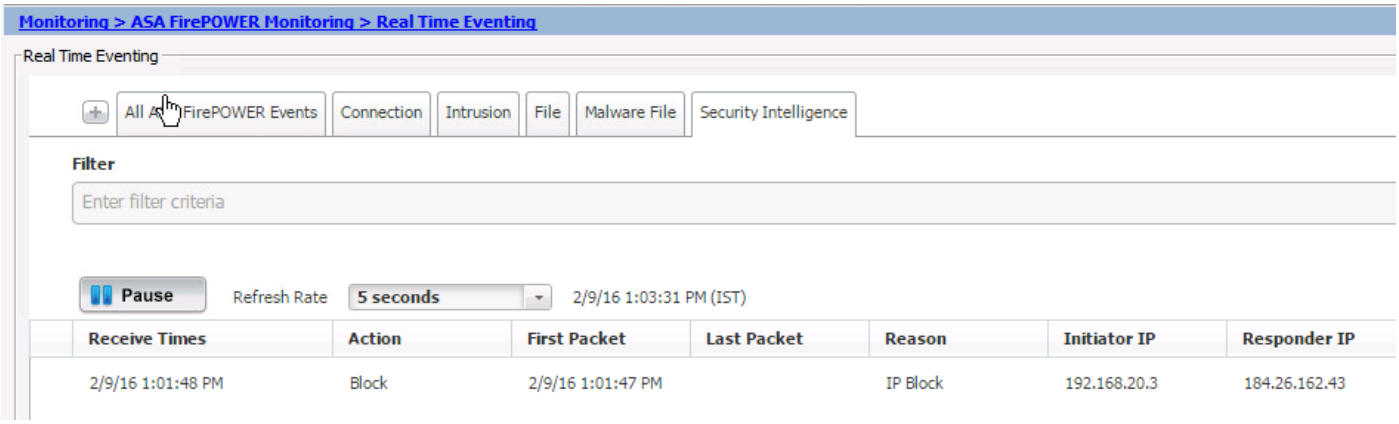


: 5.4.x [Apply ASA FirePOWER Changes]

[Monitoring] > [**ASA Firepower Monitoring] > [Task Status]**

Security Intelligence のイベントのモニタリング

Security Intelligence を FirePOWER モジュールで標示するには、[Monitoring] > [ASA Firepower Monitoring] > [Real Time Eventing] に移動します。.[Security Intelligence] タブを選択します。次の図に示すように、イベントが表示されます。

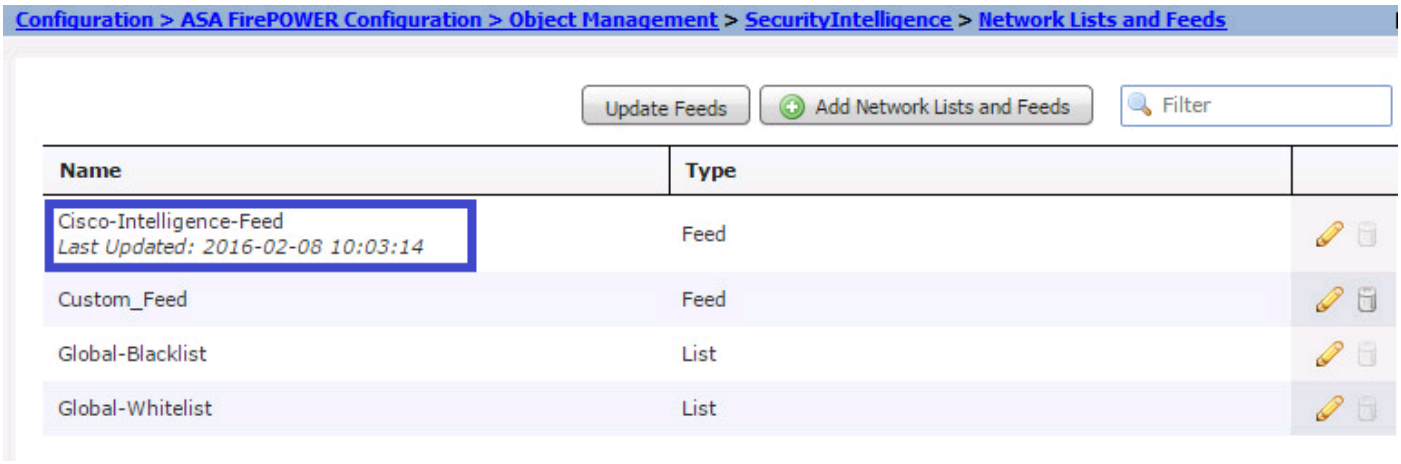


確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

Security Intelligence フィードが最新のものであることを確認するには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、フィードが最後に更新された時刻を調べます。フィードの更新頻度を設定するには、[Edit] ボタンをクリックします。



アクセス コントロール ポリシーが正常に導入されたことを確認します。

Security Intelligence をモニタして、トラフィックがブロックされているかどうかを確認します。

- Cisco ASA FirePOWER
- – Cisco Systems