目次

概要

この資料はブラックリストに載せる IP の Ciscoセキュリティ 知性/IP アドレス評判および設定を（ブロッキング）間、低い評判 IP アドレスの使用カスタム/オート・ フィード説明したものです。

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（適応性があるセキュリティ アプライアンス モデル）ファイアウォールのナレッジ、ASDM（適応性がある Security Device Manager）
- FirePOWER アプライアンス ナレッジ

:

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 を実行する ASA FirePOWER モジュール（ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X）以上に
- ソフトウェア バージョン 6.0.0 を実行する ASA FirePOWER モジュール（ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X）以上に

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

Ciscoセキュリティ 知性は悪い評判があるために Cisco TALOS チームによって判別される IP アドレスの複数の定期的にアップデートされた収集で構成します。 Cisco TALOS チームはどの悪意のあるアクティビティでも不正侵入先祖などを phishing スパム、malware のようなそれらの IP アドレスから起きる場合低い評判を判別します

Cisco IPセキュリティ 知性供給は攻撃者のデータベースを、Bogon、Bots、CNC、Dga、ExploitKit、Malware、Open_proxy、Open_relay、Phishing、応答、疑わしい スパム トラッキングします。 火力モジュールは低い評判 IP アドレスのカスタム供給を作成するオプションを提供します。

安全保障局供給の外観

安全保障局の異なるカテゴリとして分類することができる IP アドレス収集の種類についてのもう少しの情報はここにあります。

攻撃者: 脆弱性のために絶えずスキャンするか、または他のシステムを不正利用するように試みている IP アドレスの収集。

Malware: malware を伝搬させるように試みるか、またはアクティブにそれらを参照するだれでも攻撃している IP アドレスの収集。

Phishing: アクティブに ユーザ名 および パスワードのような入力機密 情報にエンドユーザをトリックするように試みているホストの収集。

スパム: ようにスパム 電子メール メッセージの送信のもと識別されたホストの収集。

Bots: botnet の一部として積極的に加わっているホストの収集は既知 bots ネット コントローラによって、制御されて。

CNC: 既知 Botnet の制御サーバとして識別されたホストの収集。

OpenProxy: 開いた Web プロキシを実行し、匿名 Web ブラウジング サービスを提供するために知られているホストの収集。

OpenRelay: サービスを中継で送る匿名電子メールを提供するために知られているホストの収集はスパムおよび phishing 攻撃者によって使用しました。

TorExitNode: 岩山 Anonymizer ネットワークのための Exit ノード サービスを提供するために知られているホストの収集。

Bogon: 割り当てられないが、送信 して います IP アドレスの収集はトラフィックを。

疑わしい: 不審 な 行動を表示する、アクティブな調査の下にある IP アドレスの収集。

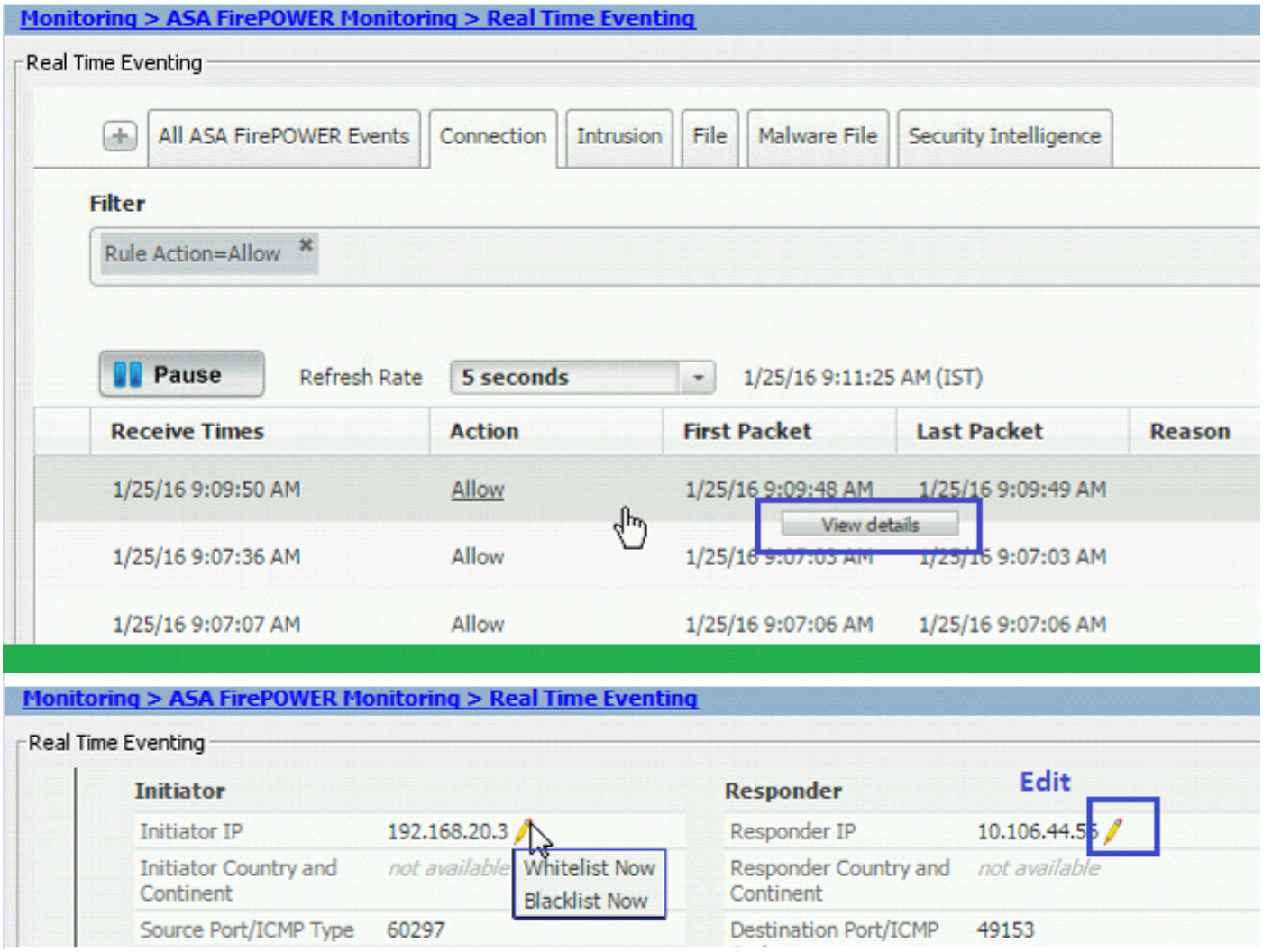
response： 繰り返し疑わしい ですか悪意のある動作で実行されて観察された IP アドレスの収集。

手動で IP アドレス グローバル ブラックリストおよびグローバル ホワイトリストを追加して下さい

火力モジュールは彼らは悪意のあるアクティビティの一部であることを確認するときある特定の IP アドレス グローバル ブラックリストを追加することを可能にします。 IP アドレスはまたグローバル ホワイトリストにブラックリスト IP アドレスによってブロックされるある特定の IP アドレスにトラフィックを許可したいと思う場合追加することができます。 IP アドレス グローバル ブラックリスト/グローバル ホワイトリストを追加する場合、ポリシーを適用する必要なしですぐに実施されます。

IP アドレス グローバル ブラックリスト グローバル ホワイトリストを追加するために、**モニタリングに > ASA FirePOWER モニタリング > リアルタイム Eventing** ナビゲート し、マウス接続イベントの浮かび、**詳細を**『View』 を選択 して下さい。

グローバル ブラックリスト グローバル ホワイトリストにソースか宛先 IP アドレスを追加できます。 ボタンを**『Edit』 をクリック し、イメージに示すようにそれぞれリストに IP アドレスを、追加するためにホワイトリスト今/ブラックリスト今**選択して下さい。



ソースか宛先 IP アドレスがグローバル ブラックリスト グローバル ホワイトリストに追加されることを確認するために、**設定 > ASA 火力設定 > オブジェクト 管理 > Security 知性 > Network Lists** にナビゲート し、グローバル **ブラックリストをグローバル な ホワイトリスト入れ**、編集します。 またリストから IP アドレスを削除するのに Delete ボタンを使用できます。

ブラックリスト IP アドレスのカスタム リストを作成して下さい

火力はブラックリストに載せることで使用することができるカスタム ネットワーク/IP アドレス リストを作成することを可能にします (ブロッキング)。 これをする 3 オプションがあります:

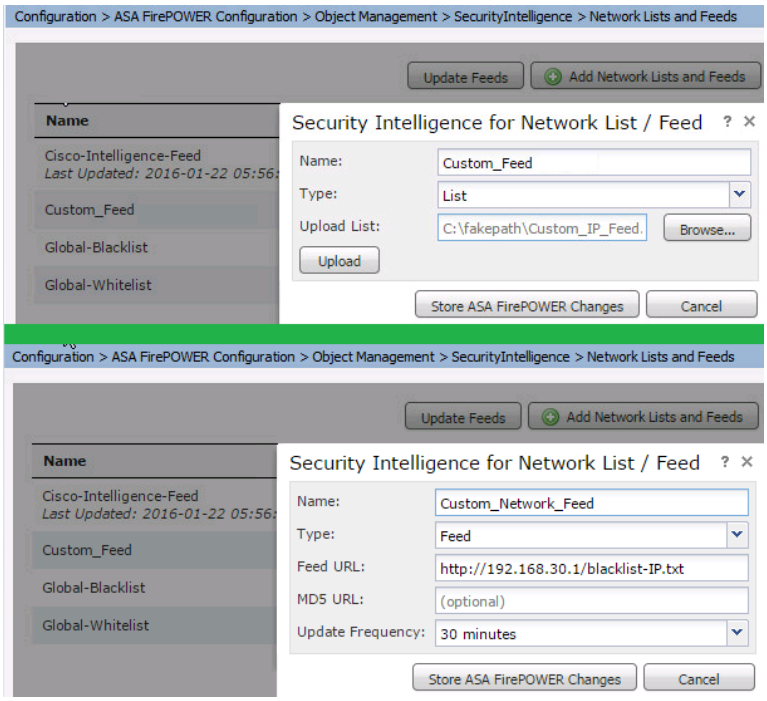
1. テキストファイル (行毎に 1 IP アドレス) に IP アドレスを書き、火力モジュールにファイルをアップロードできます。 ファイルを、ナビゲート **> オブジェクト 管理 > Security 知性 > Network Lists および供給設定 > ASA FirePOWER 設定**にアップロードし、次に**ネットワークリストおよび供給を**『Add』 をクリック するため **[Name]:** カスタム リストの名前を規定 して下さい。 **Type:** ドロップダウン リストからの選択リスト。 **アップロード リスト:** システムでテキストファイルを取付けるために『Browse』 を選択 して下さい。 ファイルをアップロードするために**アップロードを**『Option』 を選択 して下さい。
2. IPアドレスリストを取出すために火力モジュールがサード パーティ サーバを接続するカスタム リストのためにサード パーティ IP データベースを使用できます。 これを、ナビゲート **> オブジェクト 管理 > Security 知性 > Network Lists および供給設定 > ASA FirePOWER 設定**に設定し、次に**ネットワークリストおよび供給を**『Add』 をクリック するため **[Name]:** カスタム供給の名前を規定 して下さい。

   Type: ドロップダウン リストからの**供給を**『Option』 を選択 して下さい。

   供給 URL: 火力モジュールが接続される必要がある規定 し、供給をダウンロードして下さいサーバの URL を。

   MD5 URL: 供給 URL パスを検証するためにハッシュ 値を規定 して下さい。

   アップデート 周波数: システムが URL 供給サーバに接続するタイムインターバルを規定 して下さい。



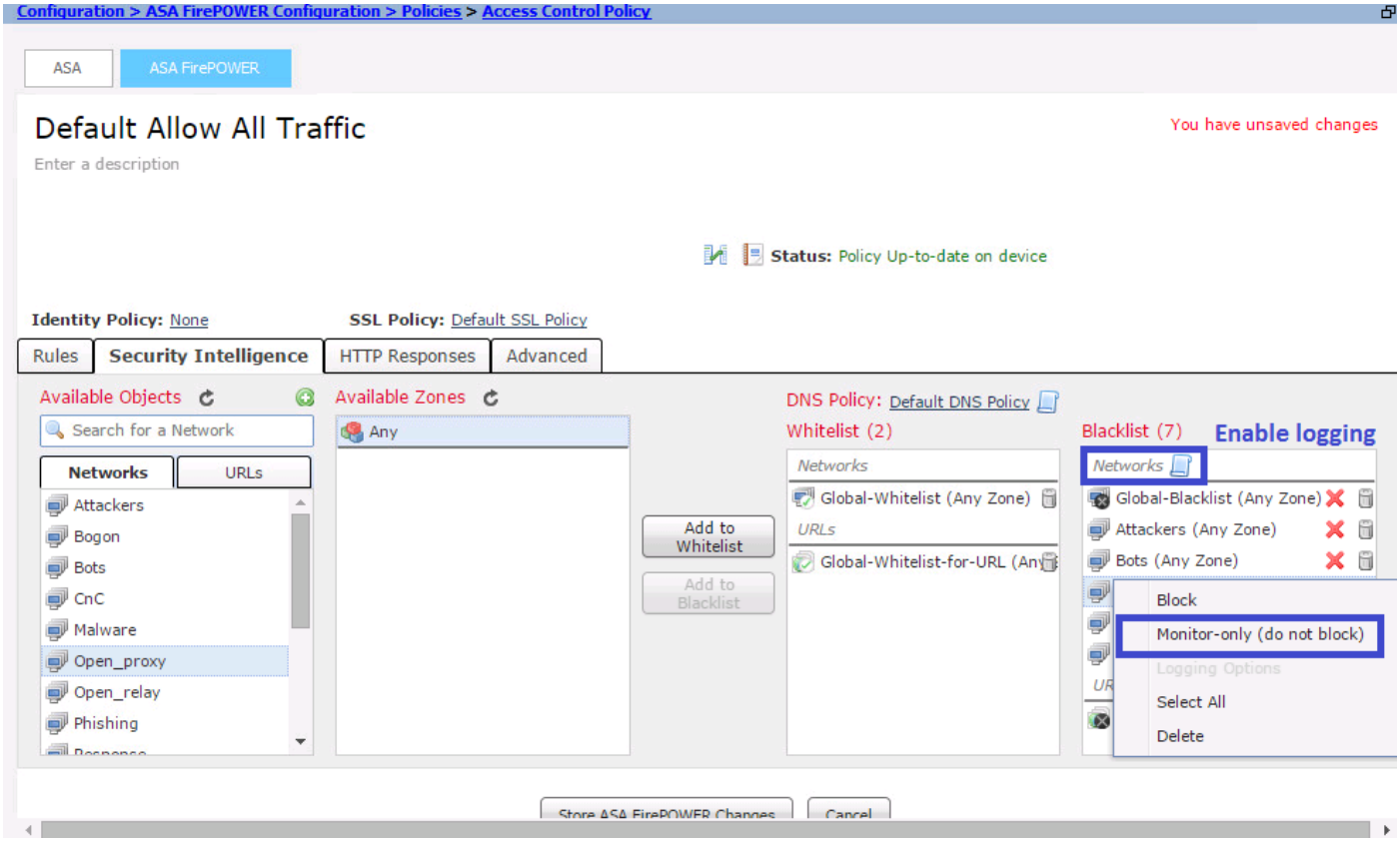
安全保障局を設定して下さい

安全保障局を設定するために、**設定 > ASA 火力設定 > ポリシー > アクセスコントロール ポリシー**に、『Security』 を選択 します **知性**タブをナビゲート して下さい。

Whitelist/ブラックリスト カラム/ブロックにネットワーク 利用可能 な オブジェクトから供給を、移動割り当てるために悪意のある IP アドレスへの接続選択して下さい。

アイコンをクリックし、イメージで指定どおりにロギングを有効に することができます。

ちょうど接続をブロックするかわりに悪意のある IP 接続のためのイベントを生成したいと思う場合供給を、選択しますイメージに示すように**モニタのみを (ブロックは)**、右クリックして下さい:

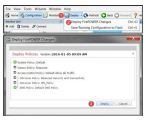


AC ポリシーの変更を保存するためにストア ASA 火力変更を『Option』 を選択 して下さい。

アクセスコントロール ポリシーを展開して下さい

変更を有効にするために、アクセスコントロール ポリシーを展開して下さい。 ポリシーを適用する前に、アクセスコントロール ポリシーはで旧式デバイスであるかどうか示す値を参照して下さい。

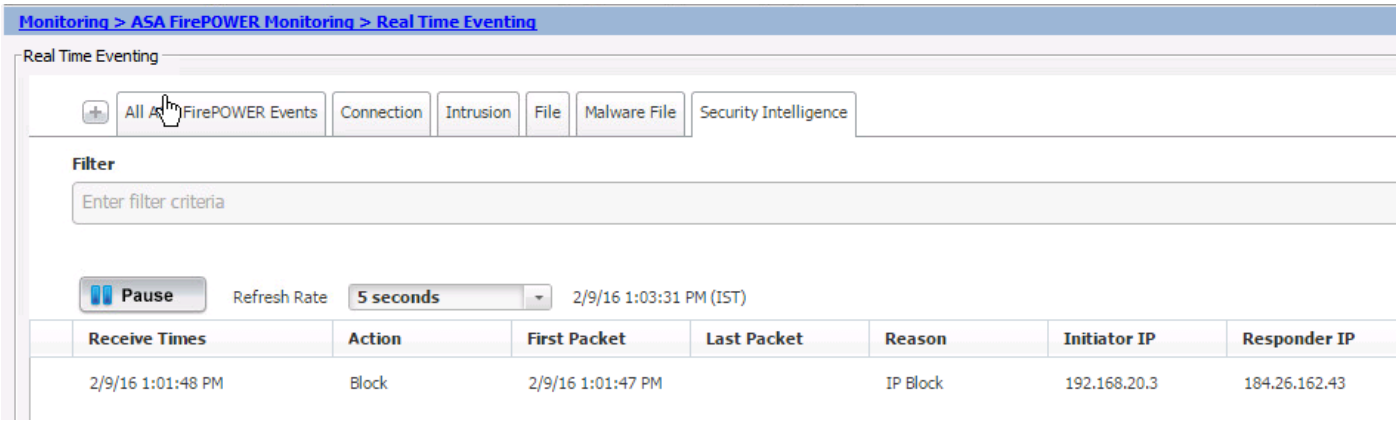
センサーへの変更を展開することはポップアップ ウィンドウで、**FirePOWER 変更を**『Deploy』 を選択 するために『Deploy』 をクリック し、それから変更を展開するために『Deploy』 を選択します。



: **> ASA >** **irePOWER** Apply

安全保障局か。s イベント モニタリング

安全保障局を、ナビゲート **モニタリング**に火力モジュールによって見るため > **ASA 火力モニタリング > リアルタイム Eventing。 安全保障局**タブを選択して下さい。 これはイメージに示すようにイベントを現れます:

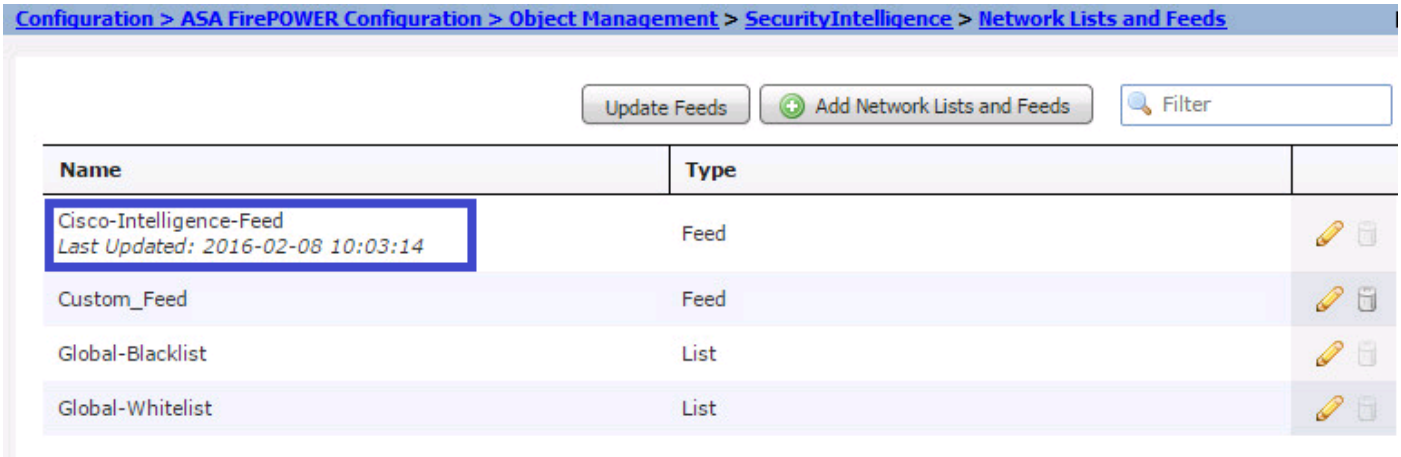


確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

安全保障局供給が最新であることを確認するために、**設定 > ASA FirePOWER 設定 > オブジェクト 管理 > Security 知性 > Network Lists** にナビゲート し、供給が最後にアップデートされた時間を**入れ**、チェックします。 供給アップデートの周波数を設定 するために Edit ボタンを選択できます。



アクセスコントロール ポリシー配備が正常に完了したようにして下さい。

トラフィックがブロックするかどうか見る安全保障局を監視して下さい。

- Cisco ASA FirePOWER
- - Cisco Systems