ASDM（オンボックス管理）を使用したFirePOWERモジュールでのドメインベースセキュリティインテリジェンス（DNSポリシー）の設定

内容

概要

このドキュメントでは、Adaptive Security Device Manager(ASDM)を使用して、ASA with FirePOWERモジュールでDomain Based Security Intelligence(SI)を設定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）ファイアウォールに関する知識
- ASDM(Adaptive Security Device Manager)
- FirePOWER モジュールの知識

注：セキュリティインテリジェンスフィルタには保護ライセンスが必要です。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- 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
- ASA FirePOWERモジュール(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)ソフトウェアバージョン6.0.0以降

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

Firepowerシステムは、DNSトラフィック要求を代行受信し、悪意のあるドメイン名を検索する機能を提供します。Firepowerモジュールが悪意のあるドメインを検出した場合、FirepowerはDNSポリシーの設定に従って要求を緩和するための適切なアクションを実行します。

IPベースのインテリジェンスに違反し、DNSロードバランス機能を悪用して、悪意のあるサーバの実際のIPアドレスを隠すように設計された新しい攻撃方法。攻撃に関連するIPアドレスは頻繁に入れ替えられ、出し入れされますが、ドメイン名はほとんど変更されません。

Firepowerは、悪意のある要求をシンクホールサーバにリダイレクトする機能を提供します。このサーバは、攻撃トラフィックに関する詳細を知るための試みを検出、偏向、または調査するためのハニーポットのサーバです。

ドメインリストとフィードの概要

[Domain Lists and Feeds（ドメインリストとフィード）]には、攻撃の種類に基づいて様々なカテゴリにさらに分類された悪意のあるドメイン名のリストが含まれます。通常、フィードは2種類に分類できます。

Cisco TALOSが提供するドメインリストとフィード

DNS攻撃者：脆弱性を継続的にスキャンしたり、他のシステムを悪用しようとするドメイン名のコレクション。

DNS Bogon：トラフィックを割り当てずに再送信するドメイン名のコレクション（別名Fake IP）。

DNSボット：ボットネットットの一部としてアクティブに参加し、既知のボットネットコントローラによって制御されるドメイン名の収集。

DNS CnC：既知のボットネットの制御サーバとして識別されるドメイン名のコレクション。

DNSエクスプロイトキット：他のシステムを悪用しようとするドメイン名のコレクション。

DNSマルウェア：マルウェアの伝播を試みる、またはマルウェアを訪れた人をアクティブに攻撃するドメイン名のコレクション。

DNS Open_proxy:Open Web Proxiesを実行し、匿名Web参照サービスを提供するドメイン名のコレクション。

DNS Open_relay：スパムやフィッシング攻撃者が使用する匿名の電子メールリレーサービスを提供するドメイン名のコレクション。

DNSフィッシング：エンドユーザーがユーザー名やパスワードなどの機密情報を入力するように積極的に操作するドメイン名のコレクション。

DNS応答：疑わしい動作や悪意のある動作で繰り返し発生するドメイン名のコレクションです。

DNSスパム：スパムメールメッセージを送信する送信元として識別されるドメイン名のコレクション。

DNSの疑い：疑わしいアクティビティを表示し、アクティブな調査中のドメイン名のコレクション。

DNS Tor_exit_node:Tor Anonymizerネットワークの終了ノードサービスを提供するドメイン名のコレクション。

カスタムドメインリストとフィード

DNSのグローバルブラックリスト：管理者によって悪意があると識別されたドメイン名のカスタムリストのコレクションです。

DNSのグローバルホワイトリスト：管理者によって本物として識別されるドメイン名のカスタムリストのコレクションです。

DNSセキュリティインテリジェンスの設定

ドメイン名ベースのセキュリティインテリジェンスを設定するには、複数の手順があります。

1. カスタムDNSフィード/リストの設定（オプション）
2. シンクホールオブジェクトの設定（オプション）
3. DNSポリシーの設定
4. アクセスコントロールポリシーの設定

5. アクセスコントロールポリシーの展開

ステップ1：カスタムDNSフィード/リストを設定します（オプション）。

ドメインを追加できる2つの定義済みリストがあります。ブロックするドメインの独自のリストとフィードを作成します。

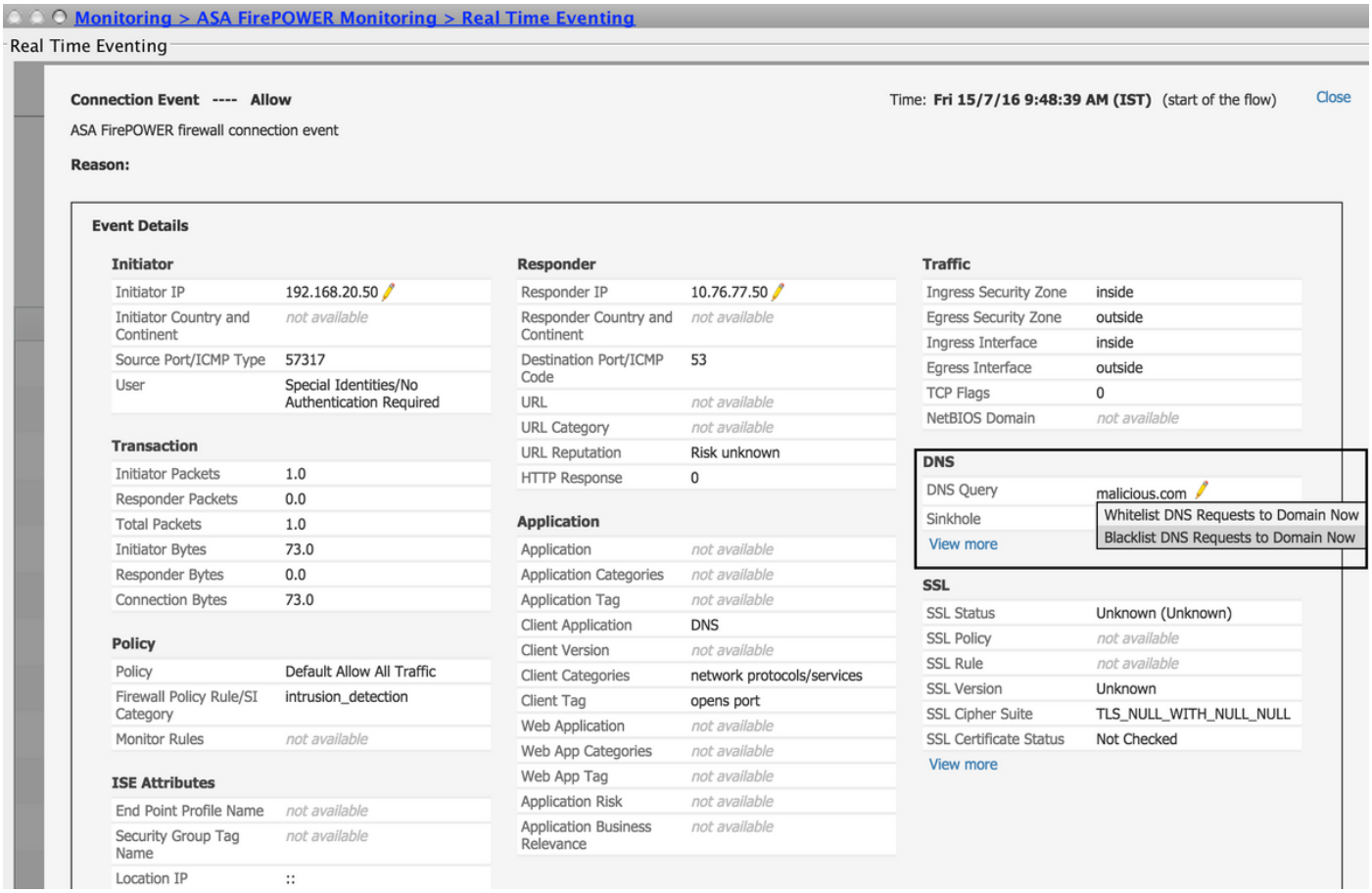
- DNSのグローバルブラックリスト
- DNSのグローバルホワイトリスト

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

Firepowerモジュールを使用すると、特定のドメインが悪意のあるアクティビティの一部であることが判明した場合に、特定のドメインをグローバルブラックリストに追加できます。ブラックリストドメインによってブロックされている特定のドメインへのトラフィックを許可する場合は、グローバルホワイトリストにドメインを追加することもできます。Global-Blacklist/Global-Whitelistにドメインを追加すると、ポリシーを適用しなくても、すぐに有効になります。

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。

ドメイン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できます。図に示すように、[DNS]セクションで**[Edit]**をクリックし、**[Whitelist DNS Requests to Domain Now/Blacklist DNS Requests to Domain Now]を選択して、ドメインをそれぞれのリストに追加します。**



ドメイン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ていることを確認す

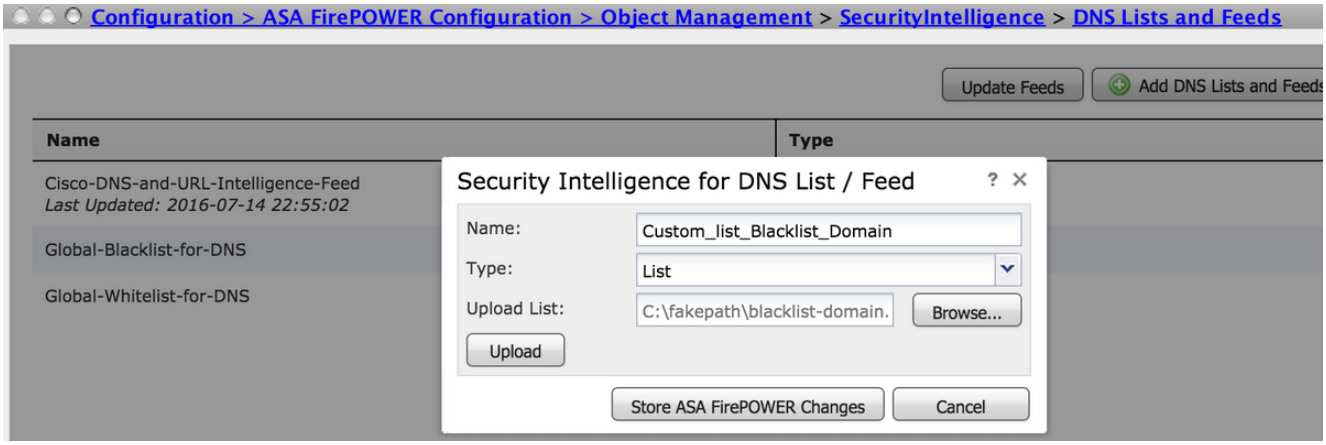
るには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [SecurityIntelligence] > [DNS Lists and Feeds]に移動し、DNS/グローバルホワイトリストを編集します。削除ボタンを使用して、リストからドメインを削除することもできます。

ブラックリストドメインのカスタムリストの作成

Firepowerを使用すると、カスタムドメインリストを作成できます。カスタムドメインリストは、2つの異なる方法でブラックリスト（ブロック）に使用できます。

1. ドメイン名をテキストファイル（1行に1つのドメイン）に書き込み、そのファイルをFirePOWERモジュールにアップロードできます。

   ファイルをアップロードするには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [SecurityIntelligence] > [DNS Lists and Feeds]に移動し、[Add DNS Lists and Feeds]を選択します　　[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。[アップロード]を選択して、ファイルをアップロードします。



   [Store ASA FirePOWER changes] をクリックして、変更内容を保存します。

2. Firepowerモジュールがサードパーティサーバを接続してドメインリストを取得できるカスタムリストには、任意のサードパーティドメインを使用できます。

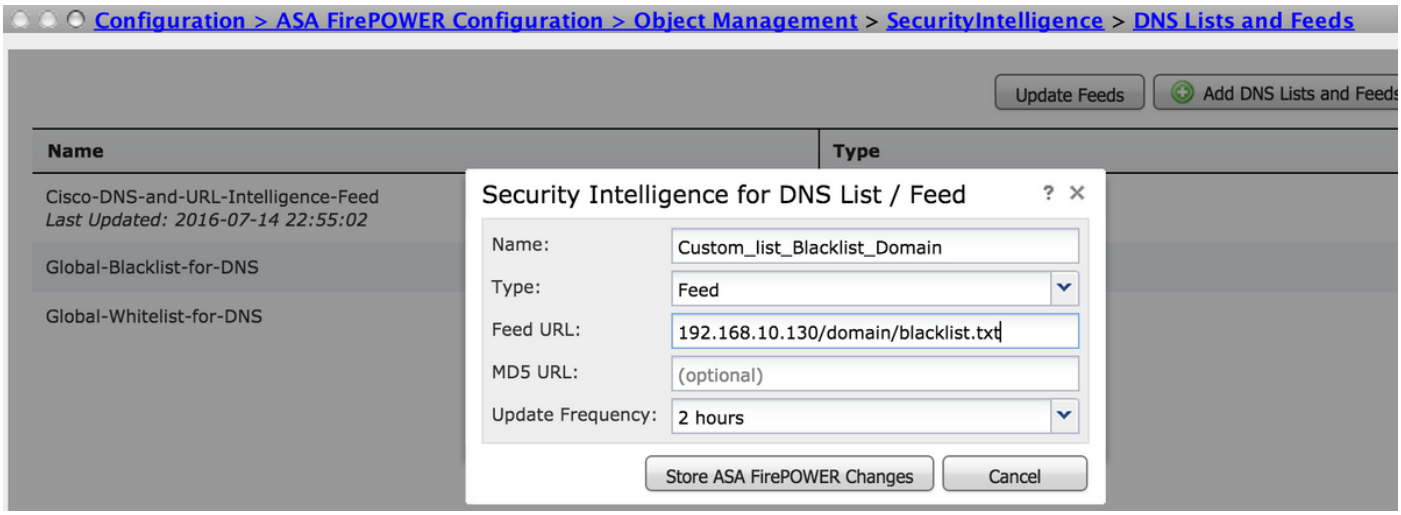
   これを設定するには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [Security Intelligence] > [DNS Lists and Feeds]に移動し、[Add DNS Lists and Feeds]を選択します
   [Name]：カスタム フィードの名前を指定します。

   Type:ドロップダウンリストから[フィード]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できるサーバ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]：モジュールがURLフィードサーバに接続する時間間隔を指定します。



[Store ASA FirePOWER Changes]を選択して、変更を保存します。

ステップ2：シンクホールオブジェクトを設定します（オプション）。

シンクホールのIPアドレスは、悪意のあるDNS要求への応答として使用できます。クライアントマシンは、悪意のあるドメインルックアップのシンクホールサーバIPアドレスを取得し、エンドマシンはシンクホールサーバへの接続を試行します。したがって、シンクホールはハニーポットとして攻撃トラフィックを調査することができます。シンクホールは、侵入のインジケータ(IOC)をトリガーするように設定できます。

シンクホールサーバを追加するには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [Sinkhole]を選択し、[Add Sinkhole]オプションをクリックします。

[Name]：シンクホールサーバの名前を指定します。

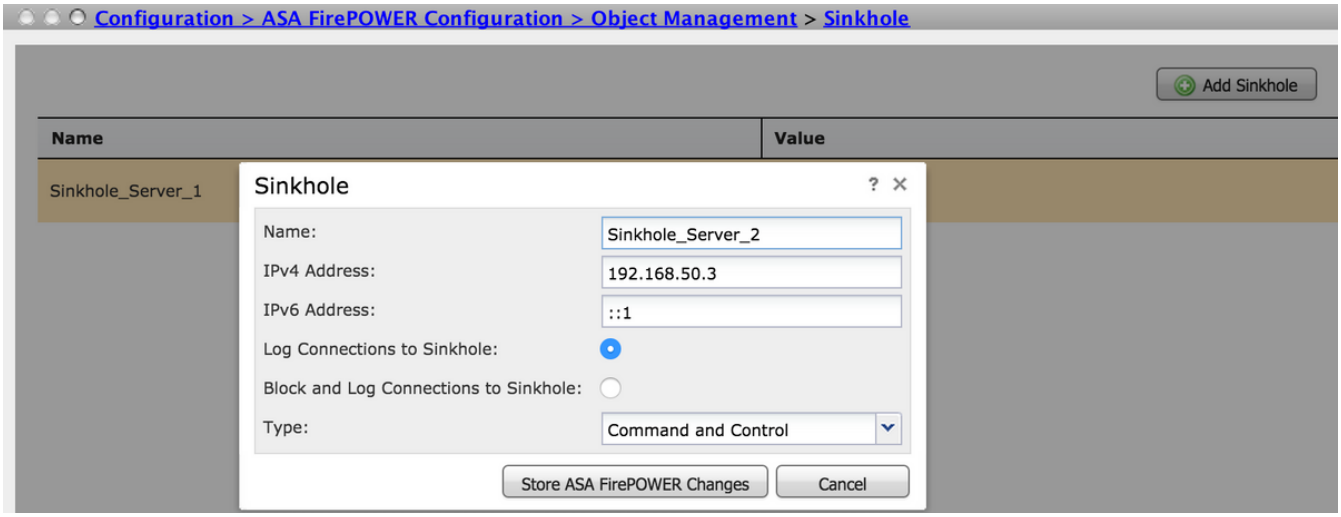
IPアドレス:シンクホールサーバのIPアドレスを指定します。

Sinkholeへの接続のログ：エンドポイントとシンクホールサーバ間のすべての接続をログに記録するには、このオプションを有効にします。

Sinkholeへの接続のブロックとログ：このオプションを有効にすると、接続がブロックされ、フロー接続の開始時にのみログが記録されます。物理シンクホールサーバがない場合は、任意のIPアドレスを指定でき、接続イベントとIOCトリガーを確認できます。

Type:シンクホールイベントに関連付けられているIOC（侵入の痕跡）のタイプを選択するドロップダウンリストからフィードを指定します。タグ付けできるシンクホールIOCには3つのタイプがあります。

- マルウェア
- コマンドと制御
- フィッシュ



ステップ3:DNSポリシーを設定します。

DNSフィード/リストのアクションを決定するには、DNSポリシーを設定する必要があります。**[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [DNS Policy]に移動します。**

デフォルトのDNSポリシーには、2つのデフォルトルールが含まれています。最初の規則である**Global Whitelist for DNS**には、許可されたドメインのカスタムリスト(**Global-Whitelist-for-DNS**)が含まれます。 このルールは、システムが任意のブラックリストドメインに一致する前に、最初に一致するように最上位に配置されます。2番目の規則である**Global Blacklist for DNS**には、ブロックされたドメインのカスタムリスト(**Global-Blacklist-for-DNS**)が含まれます。

さらにルールを追加して、**Cisco TALOS**が提供するドメインリストとフィ**ーズのさまざまなアクションを定義できます**。新しいルールを追加するには、[DNSルールの追**加]を選択します。**

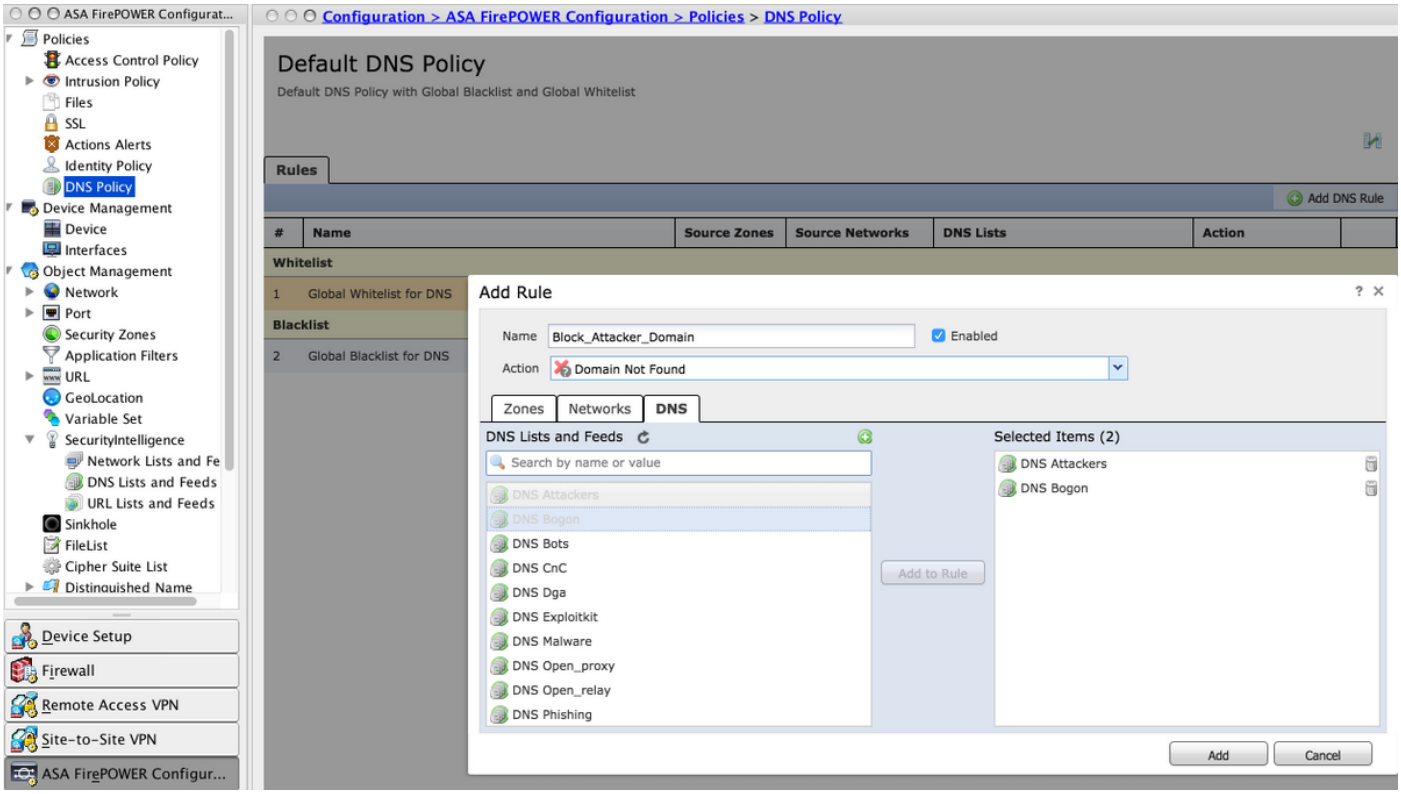
名前：ルール名を指定します。

Action: このルールが一致したときにトリガーするアクションを指定します。

- **Whitelist:**これにより、DNSクエリが許可されます。
- **モニタ:**このアクションはDNSクエリのイベントを生成し、トラフィックは後続のルールと一致し続けます。
- **ドメインが見つかりません：このア**クションは、ドメインが見つかりません（存在しないドメイン）としてDNS応答を送信します。
- **Drop**：このアクションは、DNSクエリをサイレントモードでブロックおよびドロップします。
- **シンクホール**：このアクションは、DNS要求への応答としてSinkholeサーバのIPアドレスを送信します。

ルールの条件を定**義するには、[ゾ**ーン/ネットワーク]を指定します。[DNS]タブで、**[DNS lists & Feeds]を選択**し、[Selected Items]オプションに移動します。このオプションで設定したアクションを適用できます。

組織のニーズに応じて異なるアクションを使用して、異なるDNSリストおよびフィードに対して複数のDNSルールを設定できます。

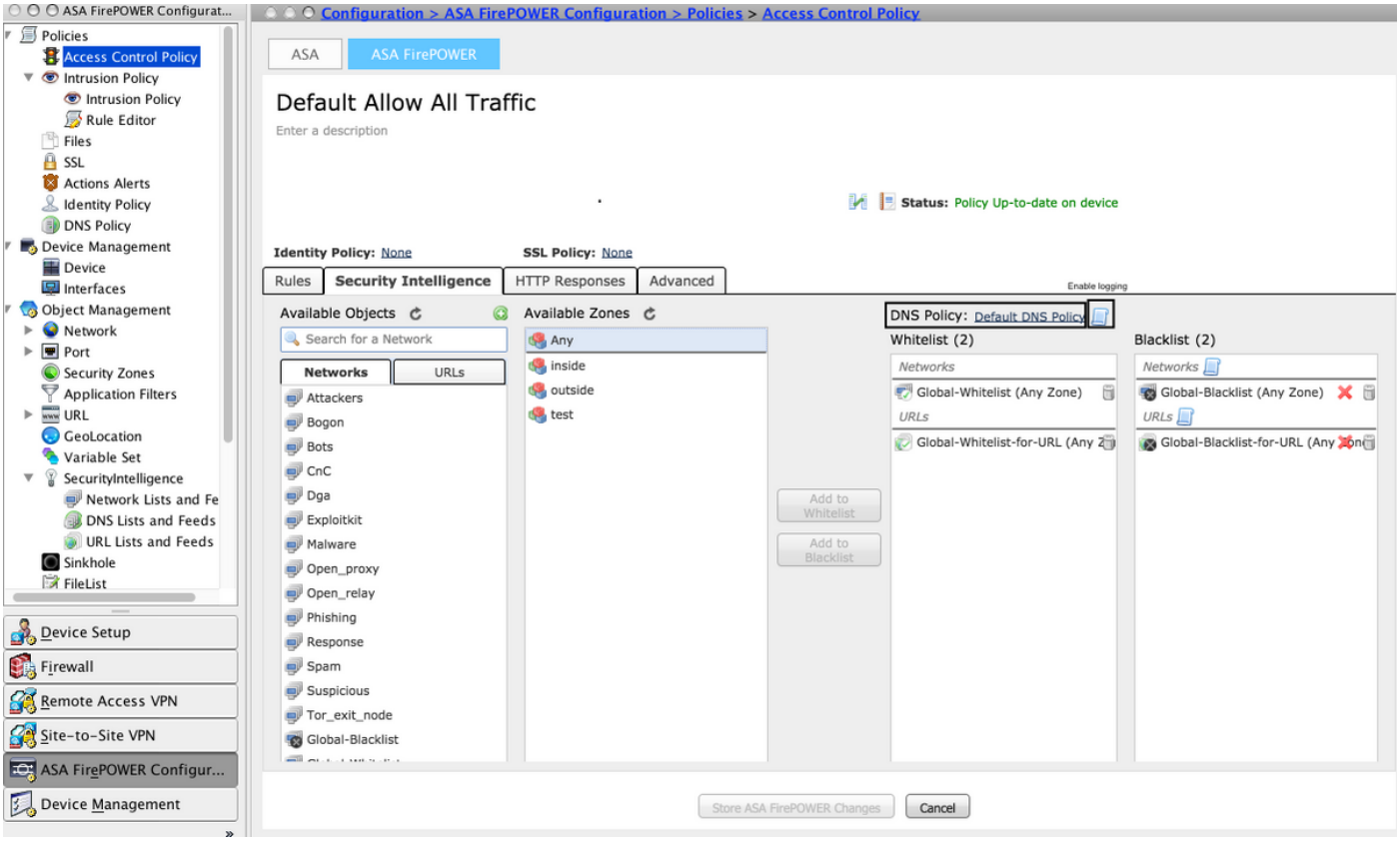


[追加]オプションをクリックして、ルールを追加します。

ステップ 4：アクセス コントロール ポリシーを設定する。

DNSベースのセキュリティインテリジェンスを設定するには、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control Policy]に移動し、[Security Intelligence]タブを選択します。

DNSポリシーが設定されていることを確認し、オプションで、図に示すように[logs]アイコンをクリックすると口グを有効にできます。



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。

ステップ5：アクセスコントロールポリシーを展開します。

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。

変更をセンサーに導入するには、[Deploy] をクリックし、[Deploy FirePOWER Changes] を選択します。これによってポップアップされるウィンドウで [Deploy] を選択すると、変更が導入されます。

> **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、**[Apply ASA FirePOWER Changes]**をクリックする必要があります。

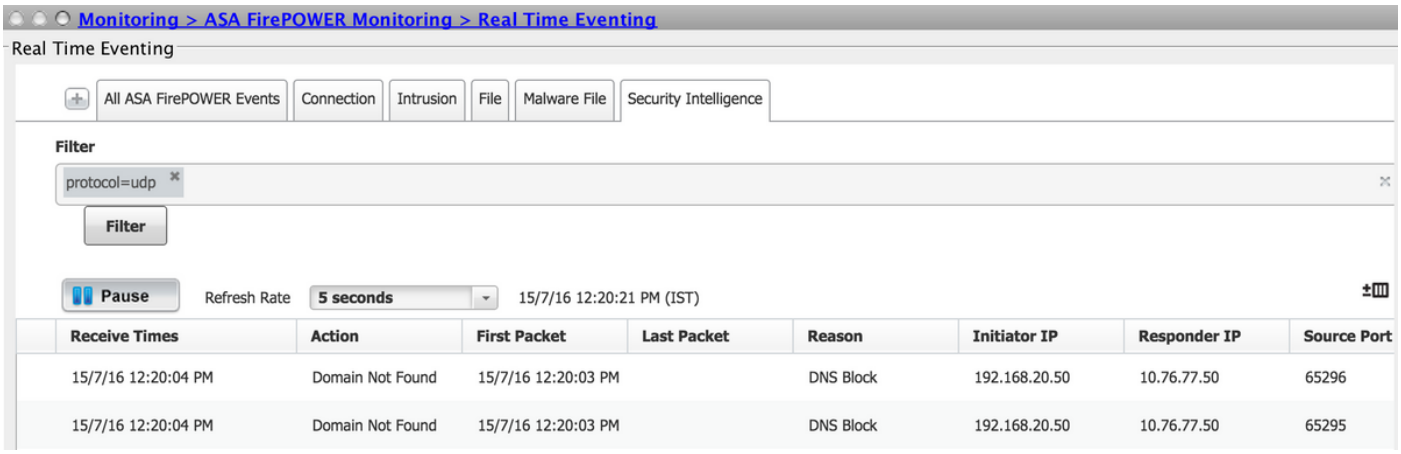
> **注**：[Monitoring] > **[ASA Firepower Monitoring] > [Task Status]に移動します。設定の変更を確認**するには、タスクが完了していることを確認します。

確認

設定は、イベントがトリガーされた場合にのみ確認できます。このため、マシン上でDNSクエリを強制的に実行できます。ただし、既知の悪意のあるサーバがターゲットになった場合には、影響に注意してください。このクエリを生成した後、[リアルタイムのイベント]セクションでイベントを確認できます。

DNSセキュリティインテリジェンスイベントモニタリング

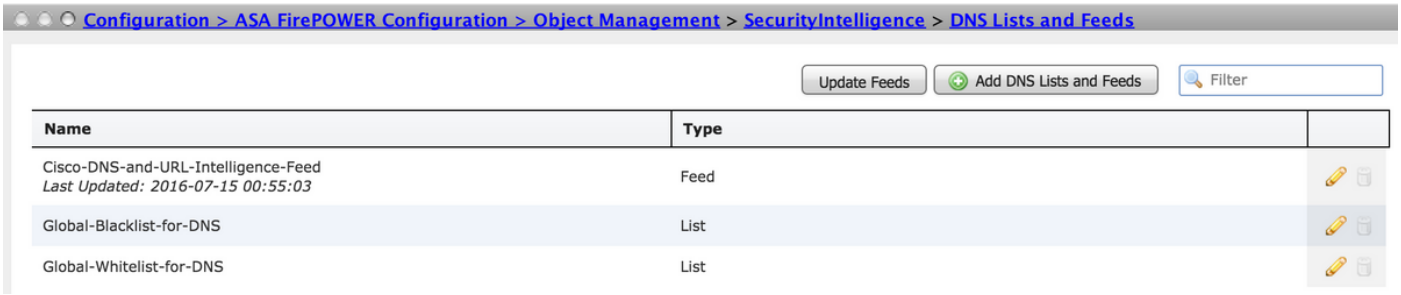
Security Intelligence を FirePOWER モジュールで標示するには、[Monitoring] > [ASA Firepower Monitoring] > [Real Time Eventing] に移動します。.[Security Intelligence] タブを選択します。次の図に示すように、イベントが表示されます。



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

セキュリティインテリジェンスフィードが最新であることを確認するには、**[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [Security Intelligence] > [DNS Lists and Feeds]に移動し、フィードが最後に更新された時刻を確認します。**[編集]を選択して、フィードの更新頻度を設定できます。



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 Real Time Eventing]タブを監視して、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。

関連情報

- Cisco ASA FirePOWER モジュール クイック スタート ガイド
- テクニカル サポートとドキュメント – Cisco Systems