

Firepower モジュール (On-Box Management) の侵入ポリシーおよびシグネチャの設定

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ 1：侵入ポリシーの設定](#)

[ステップ 1.1：侵入ポリシーの作成](#)

[ステップ 1.2：侵入ポリシーの変更](#)

[ステップ 1.3：ベース ポリシーの変更](#)

[ステップ 1.4：フィルタ バー オプションによるシグネチャ フィルタリング](#)

[ステップ 1.5：ルール状態の設定](#)

[ステップ 1.6：イベント フィルタの設定](#)

[ステップ 1.7：動的状態の設定](#)

[ステップ 2：ネットワーク解析ポリシー \(NAP \) と変数セットの設定 \(オプション \)](#)

[ステップ 3：侵入ポリシー/NAP/変数セットを含めるためのアクセス制御の設定](#)

[ステップ 4：アクセス コントロール ポリシーの導入](#)

[ステップ 5：侵入イベントの監視](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、FirePOWER モジュールの侵入防御システム (IPS) /侵入検知システム (IDS) 機能と、FirePOWER モジュールの検出ポリシーを構成するさまざまな侵入ポリシーの要素について説明示します。

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、Adaptive Security Device Manager (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。

ASA FirePOWER モジュール (ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X) で、ソフトウェア バージョン 5.4.1 以降。

ASA FirePOWER モジュール (ASA 5515-X、ASA 5525-X、ASA 5545-X、A6SA 5555-X) で、ソフトウェア バージョン 6.0.0 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。対象のネットワークが稼働中である場合には、どのような作業についても、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 IDS/IPS は、ネットワークトラフィックを検査し、ネットワーク/システム攻撃を示す悪意のあるパターン (またはシグネチャ) を特定するように設計されています。FirePOWER モジュールは、ASA のサービスポリシーが明確にモニタ モード (無差別) に設定されている場合は IDS モードで動作し、それ以外の場合はインライン モードで動作します。

FirePOWER IPS/IDS はシグネチャベースの検出方法です。IDS モードの FirePOWER モジュールはシグネチャが悪意のあるトラフィックと一致するとアラートを生成するのに対して、IPS モードの FirePOWER モジュールはアラートを生成して悪意のあるトラフィックをブロックします。

: FirePOWER [Configuration] > [ASA FirePOWER Configuration] > [License]

設定

ステップ 1 : 侵入ポリシーの設定

ステップ 1.1 : 侵入ポリシーの作成

侵入ポリシーを設定するには、Adaptive Security Device Manager (ASDM) にログインして、次の手順を実行します。

ステップ 1 : [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Intrusion Policy] に移動します。

ステップ 2 : [Create Policy] をクリックします。

ステップ 3 : 侵入ポリシーの [Name] を入力します。

ステップ 4 : 侵入ポリシーの [Description] を入力します (オプション) 。

ステップ 5 : [Drop when Inline] オプションを指定します。

ステップ 6 : ドロップダウン リストから [Base Policy] を選択します。

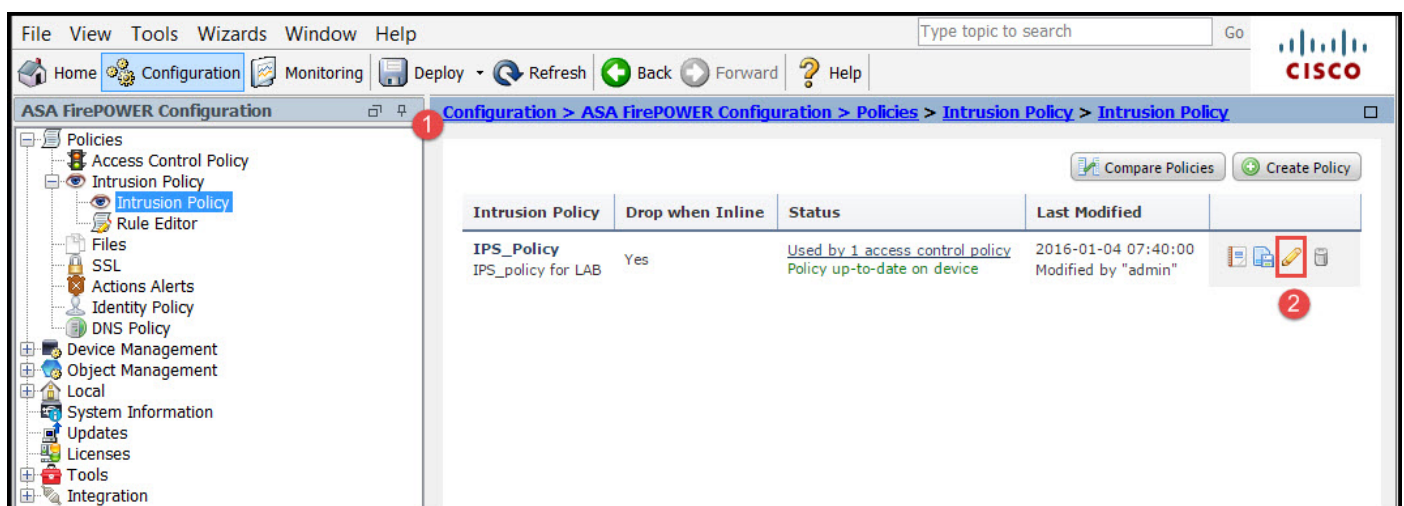
ステップ 7 : [Create Policy] をクリックして、侵入ポリシーの作成を完了します。

[Drop when Inline]

ポリシーが設定されていることはわかりますが、どのデバイスにも適用されていません。

ステップ 1.2 : 侵入ポリシーの変更

侵入ポリシーを変更するには、[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Intrusion Policy] に移動し、[Edit] オプションを選択します。



ステップ 1.3 : ベース ポリシーの変更

[Intrusion Policy Management] ページでは、[Base Policy]/[Drop when Inline]/[Save and Discard] オプションを変更できます。

ベース ポリシーには、システムが提供するいくつかの組み込みポリシーが含まれています。

1. [Balanced Security and Connectivity] : セキュリティと接続の観点から最適なポリシーです。このポリシーには有効なルールが約 7500 個あり、一部のルールはイベントを生成するだけであるのに対して、他のルールはイベントを生成するほか、トラフィックをドロップします。
2. [Security over connectivity] : セキュリティを優先させる場合は、[Security over connectivity] ポリシーを選択して、有効なルールの数を増やすことができます。
3. [Connectivity over security] : セキュリティよりも接続を優先させる場合は、有効なルールの数を減らす [Connectivity over security] ポリシーを選択できます。
4. [Maximum Detection] : このポリシーを選択すると、最大限の検出結果を得られます。
5. [No Rule Active] : このオプションはすべてのルールを無効にします。セキュリティ ポリシーに基づいて、手動でルールを有効にする必要があります。

Policy Information

Rules

Advanced Settings

Policy Layers

Policy Information < Back

Name: IPS_Policy

Description: IPS_policy for LAB

Drop when Inline:

Base Policy: Balanced Security and Connectivity (Manage Base Policy)

The base policy is up to date (Rule Update 2015-10-01-001-vrt)

This policy has 7591 enabled rules (Manage Rules)

- 114 rules generate events (View)
- 7477 rules drop and generate events (View)

This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules

Commit Changes Discard Changes

ステップ 1.4 : フィルタ バー オプションによるシグネチャ フィルタリング

ナビゲーション パネルで [Rules] オプションに移動すると、[Rule Management] ページが表示されます。ルール データベースには数千個のルールがあります。[Filter] バーは、ルールを効果的に検索するのに適した検索エンジン オプションを提供します。

[Filter] バーにキーワードを挿入すると、システムによって結果が取得されます。セキュア ソケット レイヤ (SSL) の Heartbleed 脆弱性のシグネチャを見つける要件がある場合は、フィルタバーで heartbleed というキーワードを検索して Heartbleed 脆弱性に関するシグネチャを取得できます。

ヒント : [Filter] バーに複数のキーワードが指定された場合、システムは AND ロジックを使用してそれらを組み合わせ、複合検索を作成します。

また、シグネチャ ID (SID)、ジェネレータ ID (GID)、カテゴリ ID : dos などを使用してルールを検索することもできます。

ルールは、カテゴリ/分類/Microsoft 脆弱性/Microsoft ワーム/プラットフォーム別といった、複数の方法で効果的に分割されています。ルールのこのような関連付けは、適切なシグネチャを簡単に取得し、シグネチャを効果的に調整するのに役立ちます。

また、CVE 番号を使用した検索を行って対象となるルールを見つけることもできます。次の構文を使用できます。CVE: <cve-number>

ステップ 1.5 : ルール状態の設定

ナビゲーション パネルで [Rules] オプションに移動すると、[Rule Management] ページが表示されます。ルールを選択して、[Rule State] オプションを選択し、ルールの状態を設定します。ルールに対して設定可能な状態には、次の 3 つがあります。

1. イベントの生成 : このオプションは、ルールがトラフィックに一致すると、イベントを生成します。

2. **ドロップおよびイベントの生成**：このオプションは、ルールがトラフィックに一致すると、イベントを生成してトラフィックをドロップします。
3. **無効**：このオプションはルールを無効にします。

ステップ 1.6： イベント フィルタの設定

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。 イベントが特定の回数発生するまで注意が必要ない場合もあります。 たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。 一方、ルール一致の発生回数をいくつか見るだけで、広範な問題の有無を確認できる場合もあります。

これを実現するには次の 2 つの方法があります。

1. イベントのしきい値。
2. イベント抑制。

イベントのしきい値

発生数に基づいてどのくらいの頻度でイベントを表示するかを決定するしきい値を設定できます。 イベント単位およびポリシー単位でしきい値を設定できます。

イベントのしきい値を設定する手順：

ステップ 1： イベントのしきい値を設定する [Rule(s)] を選択します。

ステップ 2： [Event Filtering] をクリックします。

ステップ 3： [Threshold] をクリックします。

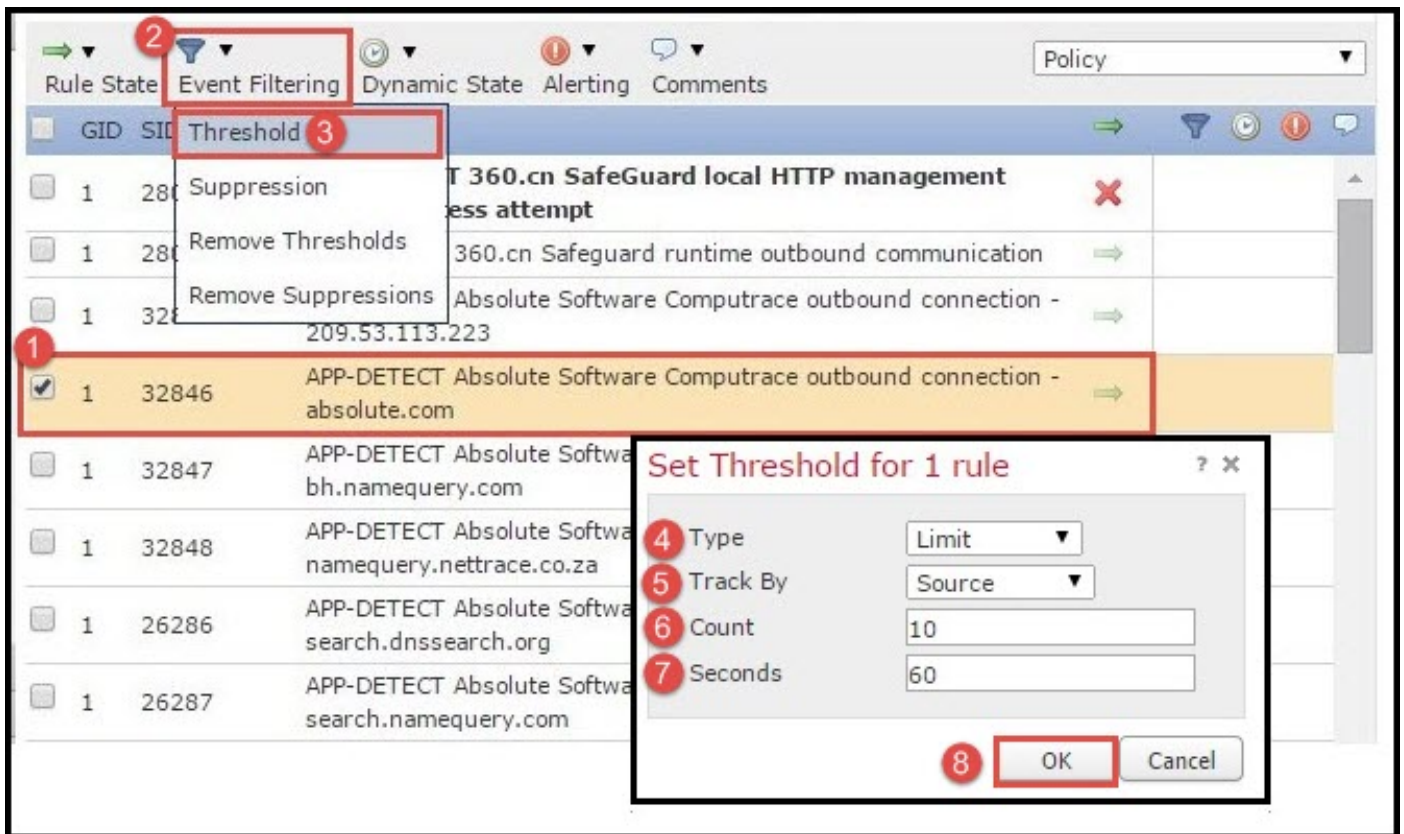
ステップ 4： ドロップダウン リストから [Type] を選択します（ [Limit] または [Threshold] のどちらかまたは両方）。

ステップ 5： [Track By] ドロップ ボックスから追跡方法を選択します（ [Source] または [Destination] ）。

ステップ 6： しきい値を満たすイベントの [Count] を入力します。

ステップ 7： カウントがリセットされるまでの [Seconds] を入力します。

ステップ 8： [OK] をクリックして完了します。



イベントのフィルタがルールに追加されると、ルールの表示の横のフィルタ アイコンが表示され、このルールに対応したイベントのフィルタリングが有効であることがわかります。

イベント抑制

指定されたイベントの通知は送信元/宛先の IP アドレスに基づいて、またはルールごとに抑制できます。

注: ルールのイベント抑制を追加する場合。シグネチャ検査は通常どおり機能しますが、トラフィックがシグネチャに一致する場合、システムはイベントを生成しません。特定の送信元/宛先を指定した場合、イベントはこのルールの特定の送信元/宛先に対してのみ表示されません。完全なルールを抑制することを選択した場合、システムはこのルールのイベントを一切生成しません。

イベントのしきい値を設定する手順：

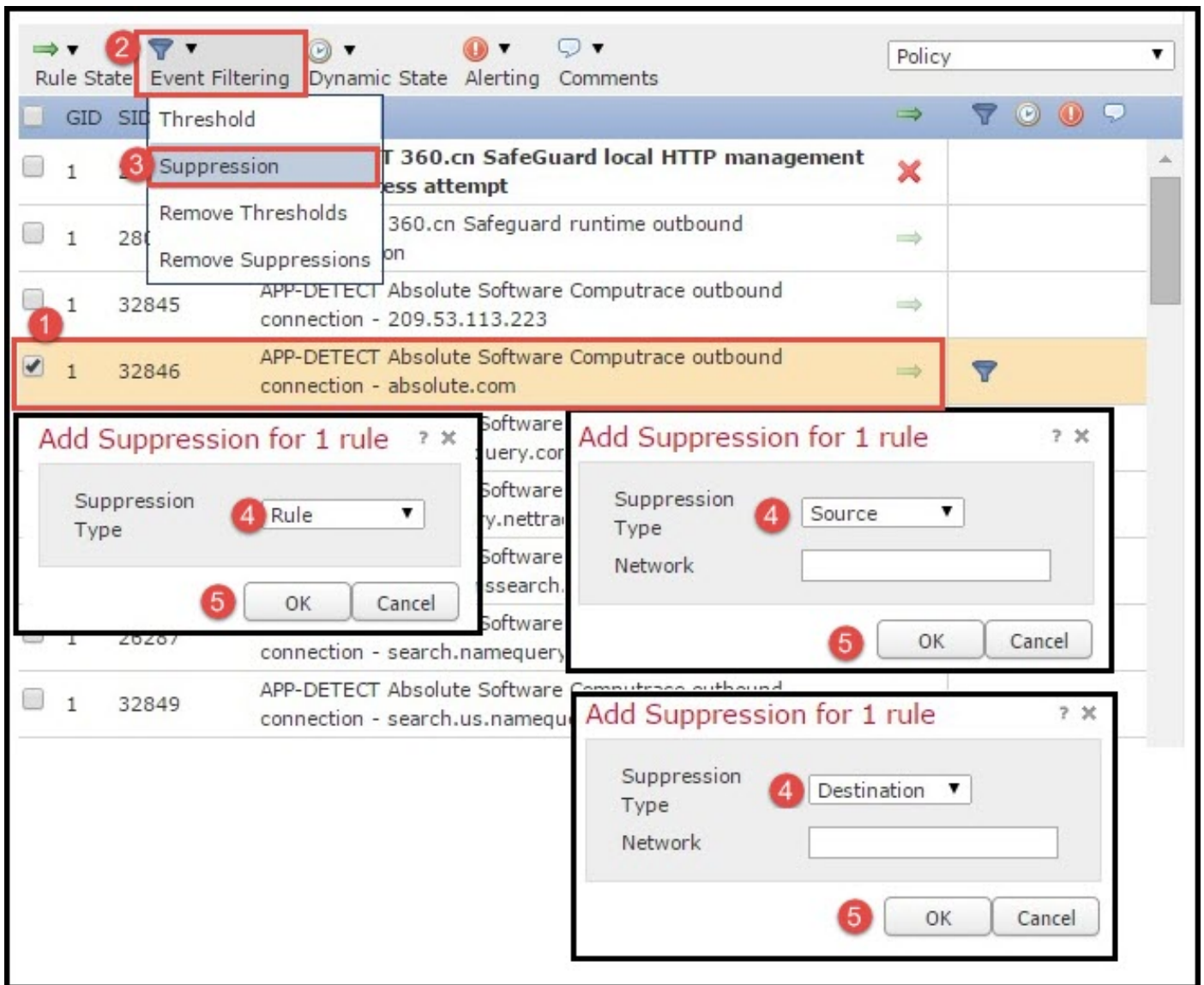
ステップ 1： イベントのしきい値を設定する [Rule(s)] を選択します。

ステップ 2： [Event Filtering] をクリックします。

ステップ 3： [Suppression] をクリックします。

ステップ 4： ドロップダウン リストから、[Suppression Type] を選択します（ [Rule] または [Source] または [Destination] ）。

ステップ 5： [OK] をクリックして完了します。



イベント フィルタがこのルールに追加されると、ルールの表示の横のフィルタ アイコンにカウント 2 と表示され、このルールに対応したイベント フィルタが 2 つ有効であることがわかります。

ステップ 1.7： 動的状態の設定

指定した条件が一致する場合にルールの状態を変更できる機能です。

パスワードを解読するブルート フォース アタックのシナリオを想定します。 シグネチャがパスワードの失敗試行を検出した場合、ルール アクションはイベントを生成します。 パスワードの失敗試行に対して、システムはアラートの生成を継続します。 この状況では、[Generate Events] のアクションを [Drop and Generate Events] に変更可能な、[Dynamic state] を使用して、ブルート フォース アタックをブロックできます。

ナビゲーション パネルで [Rules] オプションに移動すると、[Rule Management] ページが表示されます。 動的状態を有効にするルールを選択して、[Dynamic State] > [Add a Rate-based Rule State] のオプションを選択します。

レートベースのルール状態を設定する方法：

1. イベントのしきい値を設定する [Rule(s)] を選択します。
2. [Dynamic State] をクリックします。

3. [Add Rate-Based Rule State] をクリックします。
4. [Track By] ドロップ ボックスから追跡するルール状態を選択します ([Rule] または [Source] または [Destination]) 。
5. [Network] を入力します。 単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。
6. イベントの [Count] とタイムスタンプ (秒) を入力します。
7. ルールに対して定義する [New State] を選択します。
8. ルール状態が元に戻る [Timeout] を入力します。
9. [OK] をクリックして完了します。

ステップ 2 : ネットワーク解析ポリシー (NAP) と変数セットの設定 (オプション)

ネットワーク解析ポリシーの設定

ネットワーク アクセス ポリシーはプリプロセッサとも呼ばれます。 プリプロセッサはパケットを再構成し、トラフィックを正常化します。 これは不適切なヘッダー オプションの識別時に、ネットワーク層とトランスポート層のプロトコル異常を特定するのに役立ちます。

NAP は、IP データグラムの最適化を実行し、TCP ステートフル インспекションとストリーム再構成および検証チェックサムを提供します。 プリプロセッサはトラフィックを正常化し、プロトコル標準を検証および確認します。

各プリプロセッサは独自の GID 番号を持ちます。 これは、どのプリプロセッサがパケットによってトリガーされたかを表します。

ネットワーク解析ポリシーを設定するには、[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] > [Advanced] > [Network Analysis and Intrusion Policy] に移動します。

デフォルトのネットワーク解析ポリシーは、最適な推奨ポリシーである「セキュリティと接続性のバランス」です。 その他に、ドロップダウン リストから選択できるシステム提供の NAP ポリシーが 3 つあります。

カスタムの NAP ポリシーを作成するには、[Network Analysis Policy] リスト オプションを選択します。

変数セットの設定

変数セットは、送信元および宛先のアドレスおよびポートを識別するために侵入ルールで使用されます。 ルールは、変数がユーザのネットワーク環境をより正確に反映する場合に、より効率的になります。 変数は、パフォーマンス チューニングで重要な役割を果たします。

変数セットは、デフォルトのオプション (ネットワーク/ポート) で設定済みです。 デフォルト設定を変更するには、新しい変数セットを追加します。

変数セットを設定するには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [Variable Set] に移動します。 [Add Variable Set] オプションを選択して、新しい変数セットを追加します。 変数セットの [Name] を入力し、[Description] を指定します。

何らかのカスタム アプリケーションが特定のポートで動作する場合は、[Port number] フィールド

ドでポート番号を定義します。 ネットワーク パラメータを設定します。

\$Home_NET は内部ネットワークを指定します。

\$External_NET は外部ネットワークを指定します。

ステップ 3： 侵入ポリシー/NAP/変数セットを含めるためのアクセス制御の設定

[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control Policy] に移動します。 次の手順を実行する必要があります。

1. 侵入ポリシーを割り当てるアクセス ポリシー ルールを編集します。
2. [Inspection] タブを選択します。
3. ドロップダウン リストから [Intrusion Policy] を選択し、ドロップダウン リストから [Variable Sets] を選択します。
4. [Save] をクリックします。

侵入ポリシーがこのアクセス ポリシー ルールに追加されます。 シールド アイコンが金色で表示され、侵入ポリシーが有効になっていることを示します。

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

ステップ 4： アクセス コントロール ポリシーの導入

ここで、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は、アクセス コントロール ポリシーがデバイス上で期限切れになっていることがわかります。 変更をセンサーに導入するには、次の操作を行います。

1. [Deploy] をクリックします。
2. [Deploy FirePOWER Changes] をクリックします。
3. ポップアップ ウィンドウで [Deploy] をクリックします。

: 5.4.x [Apply ASA FirePOWER Changes]

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

ステップ 5： 侵入イベントの監視

FirePOWER モジュールによって生成された侵入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

ステップ 1： ルールのルール状態が適切に設定されていることを確認します。

呼び出します。正しい IPS 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。

ステップ 3 変数セットが正しく設定されていることを確認します。変数セットが正しく設定されていない場合、シグネチャはトラフィックと一致しません。

ステップ 4 アクセス コントロール ポリシーの導入が正常に完了したことを確認します。

ステップ 5： 接続イベントおよび侵入イベントを監視して、トラフィック フローが正しいルールに一致するかを確認します。

- Cisco ASA FirePOWER
- – Cisco Systems