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

# 内容

概要 前提条件 要件 使用するコンポーネント 背景説明 コンフィギュレーション 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を使用したシグニ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:ダイナミックステートの設定 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<u>ルシュート</u> 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あることが推奨されます。

\* 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いています。

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。

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 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

# 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はシグニチャベースの検出アプローチです。IDSモードの FirePOWERmoduleは、シグニ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し、 IPSモードのFirePOWERモジュールは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]

# コンフィギュレーション

### 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

| <u>File View Tools Wizards Window H</u> elp   |  | Type topic to search                       | Go alaala            |
|---|--|--|----------------------|
| 🚳 Home 🦓 Configuration 🔯 Monitoring 🔲 Save ASA Changes  | Refresh 🔇 Back 🔘 Forward 🢡 Hel                           | p  | CISCO                |
| ASA FirePOWER Configuration 🛛 🕤 🚺 Configuration   | n > ASA FirePOWER Configuration > Policies               | > Intrusion Policy > Intrusion Policy      |                      |
| Policies     Policies     Access Control Policy     Intrusion Policy     Rule Editor     Files     Actions Alarts | o policies defined. Click Create Policy to create a poli | Compare Polic 2                            | Create Policy        |
| Identity Policy   | Create Intrusion Policy                                  | ?  | ×                    |
| Divise Management   | Policy Information Name *  (3) IPS_Policy                |  |                      |
| Local   | Description 4 IPS_policy fc                              | r LAB                                      |                      |
| Icenses<br>⊕  | Drop when Inline 5 C<br>Base Policy 6 Balanced Set       | curity and Connectivity                    |                      |
| Device Setup  | * Required   | Create Policy Create and Edit Policy Cance |                      |
| Firewall  |  |  |                      |
| Remote Access VPN   |  |  |                      |
| Site-to-Site VPN  |  |  |                      |
| ASA FirePOWER Configuration   |  |  |                      |
| Device Management   |  |  |                      |
| »<br>•  |  |  |                      |
|   | <admin> 15</admin>                                       | 🕠 🗾 🔒 1,                                   | /4/16 1:17:37 AM UTC |

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。

| onfiguration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy □ |                  |   |  |         |  |  |  |  |  |  |  |
|---|------------------|---|--|---------|--|--|--|--|--|--|--|
| Create Policies   |                  |   |  |         |  |  |  |  |  |  |  |
| Intrusion Policy  | Drop when Inline | Status  | Last Modified                              |         |  |  |  |  |  |  |  |
| IPS_Policy<br>IPS_policy for LAB  | Yes              | <u>No access control policies use this policy</u><br>Policy not applied on device | 2016-01-04 07:40:00<br>Modified by "admin" | 0 🕞 🔁 🔁 |  |  |  |  |  |  |  |
| IPS_policy for LAB  |                  | Poincy not applied on device  | Modified by admin                          |         |  |  |  |  |  |  |  |

## 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。

- セキュリティと接続のバランス:セキュリティと接続の面で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する場合は、有効なルールの数を増やす Security over connectivityポリシーを選択できます。
- セキュリティ上の接続:セキュリティではなく接続を優先する場合は、有効なルールの数を 減らすセキュリティポリシー上の接続を選択できます。
- 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 🖄         | Policy Information   | < Back                             |  |  |  |  |  |
|------------------------------|--|------------------------------------|--|--|--|--|--|
| Rules<br>⊕ Advanced Settings | Name IPS_Policy Description IPS_policy for LAB   |                                    |  |  |  |  |  |
| ⊕ Policy Layers              | Drop when Inline   |                                    |  |  |  |  |  |
|                              | Base Policy        ✓       Manage Base         Balanced Security and Connectivity       ▼       ✓       ✓         ✓       The base policy is up to date (Rule Update 2015-10-01-001-vrt)       ✓ |                                    |  |  |  |  |  |
|                              | <ul> <li>➡ This policy has 7591 enabled rules</li> <li>➡ 114 rules generate events</li> <li>X 7477 rules drop and generate events</li> </ul>   | 🖉 Manage Rules<br>🔍 View<br>🔍 View |  |  |  |  |  |
|                              | This policy contains enabled preprocessor rules. Please read the rule documentation to ensure<br>the preprocessors have the correct settings for these rules                                     |                                    |  |  |  |  |  |
|                              | Commit Changes Discard Chan  | ges                                |  |  |  |  |  |

ステップ1.4:フィルタバーオプションを使用したシグニ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**:フィルタバーで複数のキーワードが使用されている場合、システムはANDロジックを使用してそれらを結合し、複合検索を作成します。

また、シグニチャ 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。

| Policy Information  | Rules                                    |  | < Back       |
|---------------------|--|--|--------------|
| Rules               | Rule Configuration                       | Filter: heartbleed   | × ?          |
| ⊕ Advanced Settings | Rule Content                             | Filter returned 33 results   |              |
| Policy Layers       | Category<br>app-detect                   | Rule State Event Filtering Dynamic State Alerting Comments                               | Policy       |
|                     | blacklist                                | 🔄 GID SID Message 🔺  | ⇒ 🕈 🕑 🕕 🖓    |
|                     | browser-chrome<br>browser-firefox        | SERVER-OTHER OpenSSL Heartbleed masscan access<br>exploitation attempt                   | × ^          |
|                     | browser-ie                               | SERVER-OTHER OpenSSL SSLv3 large heartbeat response<br>- possible ssl heartbleed attempt | * ×          |
|                     | browser-plugins                          | SERVER-OTHER OpenSSL SSLv3 large heartbeat response<br>- possible ssl heartbleed attempt | * ×          |
|                     | browser-webkit<br>content-replace        | SERVER-OTHER OpenSSL SSLv3 large heartbeat response<br>- possible ssl heartbleed attempt | * ×          |
|                     | decoder<br>exploit-kit                   | SERVER-OTHER OpenSSL SSLv3 large heartbeat response<br>- possible ssl heartbleed attempt | * ×          |
|                     | file-executable                          | SERVER-OTHER OpenSSL TLSv1 large heartbeat response<br>- possible ssl heartbleed attempt | ×            |
|                     | file-flash<br>Classifications            | SERVER-OTHER OpenSSL TLSv1 large heartbeat response<br>- possible ssl heartbleed attempt | ×            |
|                     | <b>Microsoft Vulnerabilities</b>         | SERVER-OTHER OpenSSL TLSv1 large heartbeat response                                      | ×            |
|                     | Microsoft Worms                          | - possible ssl heartbleed attempt  |              |
|                     | Platform Specific                        | - 1 30515<br>- possible ssl heartbleed attempt   | × .          |
|                     | Preprocessors                            | SERVER-OTHER OpenSSL TLSv1.1 large heartbeat   |              |
|                     | Priority                                 |  |              |
|                     | Preprocessors<br>Priority<br>Rule Update | SERVER-OTHER OpenSSL TLSv1.1 large heartbeat   | ★ 1 of 1 > 1 |

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

に移動 **ルール** ナビゲーションパネルのオプションと[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. Drop and **Generate Events: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、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。 |
|--------|-------|-------|--------|------|
|--------|-------|-------|--------|------|

| Policy Information  | Rules                                |  | < Back       |
|---------------------|--------------------------------------|--|--------------|
| Rules               | Rule Configuration                   | Filter:  | × 7          |
| ⊕ Advanced Settings | Rule Content                         | Filter returned 33 results   |              |
| ⊕ Policy Layers     | Category<br>app-detect               | Rule State Event Filtering Dynamic State Alerting Comments   | Policy       |
|                     | blacklist<br>browser-chrome          | Image: Image | × ▼ ⊙ 0 ¬    |
|                     | browser-ie<br>browser-other          | Disable ER-OTHER OpenSSL SSLv3 large heartbeat response<br>- possible ssl heartbleed attempt   | ×            |
|                     | browser-plugins                      | 1         30778         SERVER-OTHER OpenSSL SSLv3 large heartbeat response           - possible ssl heartbleed attempt  | ×            |
|                     | content-replace                      | 1         30785           SERVER-OTHER OpenSSL SSLv3 large heartbeat response           - possible ssl heartbleed attempt  | ×            |
|                     | decoder<br>exploit-kit               | SERVER-OTHER OpenSSL SSLv3 large heartbeat response<br>- possible ssl heartbleed attempt   | ×            |
|                     | file-executable                      | SERVER-OTHER OpenSSL TLSv1 large heartbeat response<br>- possible ssl heartbleed attempt   | ×            |
|                     | Classifications                      | 1         30780         SERVER-OTHER OpenSSL TLSv1 large heartbeat response           - possible ssl heartbleed attempt  | ×            |
|                     | Microsoft Vulnerabilities            | SERVER-OTHER OpenSSL TLSv1 large heartbeat response  | ×            |
|                     | Microsoft Worms<br>Platform Specific | 1 30515     SERVER-OTHER OpenSSL TLSv1 large heartbeat response     possible ss1 heartbleed attempt  | ×            |
|                     | Preprocessors                        | SERVER-OTHER OpenSSL TLSv1.1 large heartbeat   | ×            |
|                     | Rule Update                          | le<br>I  | < 1 of 1 > > |

#### 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、ルールー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。

| 1 | GID | SIL  | Threshold | 3                          |                                   |                       |                 | 4             | 9 | ۲ | 0 | 5 |
|---|-----|------|-----------|----------------------------|-----------------------------------|-----------------------|-----------------|---------------|---|---|---|---|
| 3 | 1   | 280  | Suppress  | ion                        | T 360.cn SafeG<br>ess attempt     | Guard local HTTP ma   | nagement        | ×             |   |   |   |   |
| 0 | 1   | 280  | Remove T  | hresholds                  | 360.cn Safegua                    | rd runtime outbound o | communication   | $\Rightarrow$ |   |   |   |   |
|   | 1   | 328  | Remove S  | uppressions<br>209.53.113  | Absolute Softwa<br>223            | re Computrace outbou  | nd connection - | $\Rightarrow$ |   |   |   |   |
| 0 | 1   | 3284 | 46        | APP-DETECT<br>absolute.com | <sup>•</sup> Absolute Softwa<br>n | re Computrace outbou  | nd connection - | ⇒             |   |   |   |   |
| 0 | 1   | 3284 | 47        | APP-DETECT<br>bh.nameque   | Absolute Softwa<br>ry.com         | Set Threshold f       | or 1 rule       |               | ? | × |   |   |
| 3 | 1   | 3284 | 48        | APP-DETECT<br>namequery.   | Absolute Softwa<br>nettrace.co.za | 4 Type                | Limit Source    | •<br>•        |   |   |   |   |
| 0 | 1   | 2628 | 86        | APP-DETECT<br>search.dnss  | Absolute Softwa<br>earch.org      | 6 Count               | 10              |               |   |   |   |   |
| 0 | 1   | 2628 | 87        | APP-DETECT<br>search.name  | Absolute Softwa<br>equery.com     | 7 Seconds             | 60              |               | 2 |   |   |   |

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。

| ⇒ ▼ 2 ▼ ▼<br>Rule State Event Filtering Dyr  | amic State Alerting Comments  | Policy                              |               | • |
|--|---|-------------------------------------|---------------|---|
| GID SID Threshold  |   | ⇒                                   | 7 🕑 🛈 🦻       | ) |
| 1 3 Suppression  | T 360.cn SafeGuard local HTTP management<br>ess attempt   | ×                                   |               | - |
| 1 280     Remove Thresholds     Remove Suppression   | 360.cn Safeguard runtime outbound<br>ns on  | ⇒                                   |               |   |
| 1 32845 APP-DET  | CT Absolute Software Computrace outbound<br>n - 209.53.113.223  | $\Rightarrow$                       |               |   |
| 1 32846 APP-DET     connecti   | CT Absolute Software Computrace outbound<br>n - absolute.com  |                                     | •             |   |
| Add Suppression for 1<br>Suppression<br>Type<br>5<br>0K<br>0K<br>0K<br>0K<br>1 20207<br>connecti<br>1 32849<br>APP-DET<br>connecti | ule       ? *       Software<br>uery.cor         Software<br>y.nettrai       Suppression<br>Type       Source         Software<br>y.nettrai       Suppression<br>Type       Source         Software<br>y.nettrai       Software<br>ssearch.       Network       Source         Software<br>n - search.namequery       Software       Source         Software<br>n - search.us.namequery       Source       Source         Suppression<br>n - search.us.namequery       Suppression<br>Add Suppression for 1       Suppression<br>Type         Suppression<br>n - search.us.namequery       Suppression<br>(Mathematical Suppression<br>( | rule<br>e<br>OK<br>1 rule<br>nation | ? X<br>Cancel |   |

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:ダイナミックステートの設定

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。

に移動 **ルール** オプションがナビゲーションパネルに表示され、[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-base 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行い、TCPステートフルインスペクションおよびストリーム の再構成とチェックサムの検証を行います。プリプロセッサは、トラフィックの正規化、プロト コル標準の検証、検証を行います。

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 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。

| Configuration > ASA FirePOWE     | R Configuration > Policies > Access                         | Control Policy      |   |          |   |
|----------------------------------|---|---------------------|---|----------|---|
| ASA ASA FirePOWER                |   |                     |   |          |   |
|                                  |   | -                   |   |          |   |
| Default Allow All T              | raffic  |                     |   |          |   |
| custom policy                    |   |                     |   |          |   |
|                                  |   |                     |   |          |   |
|                                  |   |                     | Status: Policy Up-to-date on device                           |          |   |
| Identity Policy: None            | SSL Policy: None  |                     |   |          |   |
| Rules Security Intellic Net      | work Analysis and Intrusion Pol                             | icies               | 2 X   |          |   |
| General Settings                 | WORK Allarysis and Inclusion For                            |                     |   | Ø        |   |
| Maximum URL characters           | rusion Policy used before Access Control<br>e is determined | No Rules Active     | Y   | No       |   |
| Allow an Interactive Bloc        | rusion Policy Variable Set                                  | Default-Set         | ▼ Ø   | ß        |   |
| Retry URL cache miss loo         | work Analysis Rules   | No Custom Rules     | Network Analysis Policy List                                  | Disabled |   |
| Inspect traffic during pol       | ault Network Analysis Policy                                | Balanced Security a | and Connectivity  | C.       |   |
| Identity Policy Setting          | avart to Defaults   |                     |   | Ø        |   |
| Identity Policy                  |   | None                |   | 5        |   |
| SSL Policy Settings              |   | A                   | Performance Statistics - Sample Time (seconds)                | 300      |   |
| SSL Policy to use for inspecting | a encrupted connections                                     | None                | Regular Expression - Limit                                    | Default  |   |
| SSEPCICY to use for inspecting   | encrypted connections                                       | none                | Regular Expression - Recursion Limit                          | Default  |   |
| Network Analysis and Intru       | usion Policies  |                     | Intrusion Event Logging Limits - Max Events Stored Per Packet | 8        | - |
|                                  |   |                     | Const   |          |   |
|                                  |   | SLOTE ASA FREEDOWL  |   |          |   |

## 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。

| ASA FirePOWER Configuration  | <u>Configuration &gt;</u>  | ASA FirePOWER             | Configurati       | on > Obje | ect Management > <u>Variable Set</u> |             |     |  |
|--|--|---------------------------|-------------------|-----------|--------------------------------------|-------------|-----|--|
| Policies     Source Management     Source Management     Source Management     Source Management     Source Management     Source Management     Source Management |  |                           |                   |           | O Add Variable Set                   | Silter      |     |  |
| Port     Security Zones  | Name   | Name Description          |                   |           |                                      |             |     |  |
| Application Filters     URL     GeoLocation  | Default-Set This Variable Set is system-provided. New Variable Set |                           |                   |           |                                      |             |     |  |
| Variable Set   | Name:  | Name: Custom_Variable_Set |                   |           |                                      |             |     |  |
| Security intelligence  | Description:   | Enter a description       | n                 |           |                                      |             | ]   |  |
| FileList   |  |                           |                   |           |                                      | 🕢 Add       |     |  |
| ⊕-¶ Distinguished Name     ⊕   | Variable N   | lame                      | Type Value        |           |                                      |             |     |  |
| Local  | Customize  | ed Variables              |                   | 23        |                                      | A           |     |  |
| Updates  | This catego  | ory is empty              |                   |           |                                      | _           |     |  |
| Elcenses   | Default Va   | ariables                  |                   |           |                                      |             |     |  |
| ⊞- <sup>™</sup> Integration  | AIM_SERVE  | RS                        | Network [64.12.3] |           | 31.136/32, 205.188.210.203/32, 6]    | <b>2</b> 36 |     |  |
|  | DNS_SERV   | ERS                       | Network           | HOME_N    | NET                                  | <b>2</b> 26 |     |  |
|  | EXTERNAL   | NET                       | Network           | any       |                                      | <b>2</b> 76 |     |  |
|  | FILE_DATA  | PORTS                     | Port              | [HTTP_I   | PORTS, 143, 110]                     | Ø98         |     |  |
| Device Setup   | FTP_PORTS  |                           | Port              | [21, 21   | 00, 3535]                            | <b>2</b> 76 |     |  |
| ᇌ Firewall   | GTP_PORTS  | 5                         | Port              | [3386,    | 2123, 2152]                          | Ø98         |     |  |
| Remote Access VPN  | HOME_NET   |                           | Network           | any       |                                      | <b>0</b> 28 | > C |  |
| Site-to-Site VPN   |  |                           |                   |           |                                      |             |     |  |
| ASA FirePOWER Configuration  |  |                           |                   |           |                                      |             |     |  |
| Device Management  |  |                           |                   |           | Store ASA FirePOWER Changes          | Cancel      |     |  |
|  |  |                           |                   |           |                                      |             |     |  |

## 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。

| tandard Rules         |            |              |        |               |              |             |           |               |               |          |
|-----------------------|------------|--------------|--------|---------------|--------------|-------------|-----------|---------------|---------------|----------|
| Access_Policy_Rule    | any        | any          | any    | any an        | y any        | any         | any       | any           | Allow         | VDD0     |
| ot Rules              |            |              |        |               |              |             |           |               |               | 0        |
|                       |            |              |        |               |              |             |           |               |               |          |
| diting Rule - Acces   | s_Policy_R | ule          |        |               |              |             |           |               |               | ?        |
|                       |            |              |        |               |              |             |           |               |               |          |
| Name Access_Policy_Ru | le         |              |        | ✓ E           | nabled       |             | Move      |               |               |          |
| Action 🖌 Allow        |            |              | ▼ IP:  | 5: IPS_Policy | Variables: D | Default-Set | Files: no | inspection Lo | ogging: no la | ogging   |
|                       | r          |              |        |               | γ            |             |           |               | 7             | r        |
| Zones Networks        | ▲ Users    | 🔺 Applicatio | ns Por | ts 🔺 URLs     | 🔺 ISE At     | ttributes   |           | Inspection    | Logging       | Comments |
| trusion Policy        |            |              |        |               |              | Variable    | Set       |               |               |          |
| PS_Policy             |            |              |        |               | × 🖉          | Default     | Set       |               |               |          |
|                       |            |              |        |               |              |             |           |               |               |          |
| le Policy             |            |              |        |               |              |             |           |               |               |          |
| None                  |            |              |        |               |              |             |           |               |               | *        |
|                       |            |              |        |               |              |             |           |               |               |          |
|                       |            |              |        |               |              |             |           |               |               |          |
|                       |            |              |        |               |              |             |           | 4             | Save          | Cancel   |

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

| M 📑 Status: Access Control policy out-of-date on device |                         |                 |                      |                    |                  |             |            |             |                  | ce         |                        |            |      |
|---|-------------------------|-----------------|----------------------|--------------------|------------------|-------------|------------|-------------|------------------|------------|------------------------|------------|------|
| Ide   | ntity Policy: <u>No</u> | <u>1e</u>       | SSL Policy: <u>N</u> | lone               |                  |             |            |             |                  |            |                        |            |      |
| Ru  | les Security            | intelligence    | HTTP Responses       | Advanced           |                  |             |            |             |                  |            |                        |            |      |
|   |                         |                 |                      |                    |                  |             |            | 💿 Add Ca    | tegory 📀 A       | dd Rule    | Search Rules           |            | ×    |
| #   | Name                    | Source<br>Zones | Dest<br>Zones        | Source<br>Networks | Dest<br>Networks | Users       | Applicat   | Src Ports   | Dest Ports       | URLs       | Action                 | V 🕞 🖉 🕫    |      |
| Adm   | Administrator Rules     |                 |                      |                    |                  |             |            |             |                  |            |                        |            |      |
| Thi   | s category is emp       | Y               |                      |                    |                  |             |            |             |                  |            |                        |            |      |
| Sta   | ndard Rules             |                 |                      |                    |                  |             |            |             |                  |            |                        |            |      |
| 1   | Access_Policy_R         | ile <i>any</i>  | any                  | any                | any              | any         | any        | any         | any              | any        | Allow                  | 0 [] [] 🤍  | a 🖉  |
| Roo   | t Rules                 |                 |                      |                    |                  |             |            |             |                  |            |                        |            |      |
| Thi   | s category is emp       | γ               |                      |                    |                  |             |            |             |                  |            |                        |            |      |
| Def   | ault Action             |                 |                      |                    |                  |             |            | Intrusion P | revention: Balar | nced Secu  | irity and Connectivity | *          | \$ 📕 |
|   |                         |                 |                      |                    |                  |             |            |             |                  |            |                        |            |      |
|   |                         |                 |                      |                    |                  |             |            |             | Displaying       | g 1 - 1 of | 1 rules  < < Pag       | e 1 of 1 > | > C  |
|   |                         |                 |                      |                    | Store            | ASA FirePOW | ER Changes | Cancel      |                  |            |                        |            |      |

[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に、 デバイスにAccess Control Policy out-of-dateと表示されます。センサーに変更を展開するには、 次の手順を実行します。

- 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。

| File View Tools Wizards Window     | Help                                       |
|------------------------------------|--|
| 🚮 Home 🦓 Configuration 🔯 Monitor 🚺 | Deploy - 🐼 Refresh 🔇 Back 🔘 Forward 🤗 He   |
| Device List                        | 2 Deploy FirePOWER Changes Ctrl+D          |
| 🕈 Add 📋 Delete 🚿 Connect           | Save Running Configuration to Flash Ctrl+S |
| Find: Go                           | North North Context                        |

| Deploy FirePOWER Changes   |                 | 2      |
|--|-----------------|--------|
| Deploy Policies Version:2016-01-05 09:09 AM  | м               | - Pro- |
| <ul> <li>System Policy: Default</li> <li>Sensor Policy: firepower</li> <li>Access Control Policy: Default Allow All Traffic</li> <li>Intrusion Policy: Balanced Security and Connectivity</li> <li>Intrusion Policy: IPS_Policy</li> </ul> |                 |        |
| W DNS POICY: Default DNS Policy  | 3 Deploy Cancel |        |

: 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表示するには、次の場所に移動します 。 [Monitoring] > [ASA FirePOWER Monitoring] > [Real Time Eventing]。

| ring > ASA FIREPOWER FIOI  | itoring > Real Time Ev                   | venting   |   |                   |  |
|--|--|---|---|-------------------|--|
| Eventing   |  |   |   |                   |  |
| Gaurav_Connection_Eve  | ents × All ASA FirePOW                   | VER Events Connection   | Intrusion                               | File Malware File | Security Intelligen                        |
| Filter   |  |   |   |                   |  |
| Rule Action=Block * reason   |  |   |   |                   |  |
| Kule Action-block Teasor   | -Intrusion brock                         |   |   |                   |  |
|  |  |   |   |                   |  |
|  |  |   |   |                   |  |
| Rauso Defeato  | Notes I for some de                      | 1/10/16 6-17  | - 42 DM (ICT)                           |                   |  |
| Pause Refresh R  | Rate <b>5 seconds</b>                    | • 1/10/16 6:13  | 3:42 PM (IST)                           |                   |  |
| <b>Pause</b><br>Refresh F  | Rate 5 seconds                           | <ul> <li>1/10/16 6:13</li> <li>Event Type</li> </ul>                | 3:42 PM (IST)                           | Inline Result     | Reason                                     |
| Pause       Refresh R         Receive Times       1/10/16 6:11:50 PM   | Rate <b>5 seconds</b> Action Block       | • 1/10/16 6:13     Event Type     ASA FirePOWER C                   | 3:42 PM (IST)<br>onnection              | Inline Result     | Reason<br>Intrusion Bloc                   |
| Pause         Refresh R           Receive Times         1/10/16 6:11:50 PM           1/10/16 6:09:52 PM         1/10/16 6:09:52 PM | Rate <b>5 seconds</b> Action Block Block | 1/10/16 6:13     Event Type     ASA FirePOWER C     ASA FirePOWER C | 3:42 PM (IST)<br>onnection<br>onnection | Inline Result     | Reason<br>Intrusion Bloc<br>Intrusion Bloc |

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

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。

ステップ2:アクセスルールに正しいIPSポリシーが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展開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