デバイス設定の管理

[デバイス管理（Device Management）] ページでは、ASA FirePOWER モジュールのデバイスおよびインターフェイスの設定を管理することができます。

注意 フェールオーバーのペアで ASA を設定した場合、ASA FirePOWER の設定は、セカンダリ デバイス上の ASA FirePOWER モジュール に自動的に同期されません。設定を変更するたびに、プライマリから ASA FirePOWER の設定を手動でエクスポートし、それをセカンダリへインポートする必要があります。

詳細については、次の項を参照してください。

デバイス設定の編集

[デバイス管理（Device Management）] ページの [デバイス（Device）] タブには、デバイスが ASA FirePOWER モジュール に適用されたときに詳細なデバイス設定と情報が表示されます。さらにこれにより、表示されるモジュール名や管理設定の変更など、デバイス設定のいくつかの部分に変更を加えることができます。

詳細については、次の各項を参照してください。

一般的なデバイス設定の編集

ライセンス:任意（Any）

[デバイス（Device）] タブの [一般（General）] セクションに表示されるモジュール名は、変更できます。ここで、デバイスがパケットを ASA FirePOWER モジュール に転送できるかどうかを指定することもできます。

一般的なデバイス設定を編集するには、次の手順を実行します。

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] の順に選択します。

[デバイス（Device）] ページが表示されます。

手順 2　[一般（General）] セクションの横にある編集アイコン（  ）をクリックします。

[一般（General）] ポップアップ ウィンドウが表示されます。

手順 3　[名前（Name）] フィールドに、モジュールに割り当てる新しい名前を入力します。英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

手順 4　パケット データをイベントと一緒に ASA FirePOWER モジュール に保存できるようにするには、[パケットの転送（Transfer Packets）] チェック ボックスをオンにします。デバイスがイベントと一緒にパケット データを送信できないようにするには、このチェック ボックスをオフにします。

手順 5　[保存（Save）] をクリックします。

これにより、変更内容が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用（3-5 ページ）を参照してください）。

デバイス システム設定の表示

ライセンス:任意（Any）

[デバイス（Device）] タブの [システム（System）] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

表 3-1　[システム (System)] セクション テーブルのフィールド

フィールド	説明
モデル	デバイスのモデル名と番号。
シリアル（Serial）	デバイスのシャーシのシリアル番号。
時刻（Time）	デバイスの現在のシステム時刻。
バージョン（Version）	ASA FirePOWER モジュールに現在インストールされているソフトウェアのバージョン。
ポリシー	ASA FirePOWER モジュール に現在適用されているシステム ポリシーへのリンク。

高度なデバイス設定について

[デバイス(Device)] タブの [詳細設定(Advanced)] セクションには、次の表に示すように、構成時の詳細設定が表示されます。

表 3-2　[詳細設定(Advanced)] セクション テーブルのフィールド

フィールド	説明
アプリケーション バイパス（Application Bypass）	モジュールでの自動アプリケーション バイパスの状態。
バイパスしきい値（Bypass Threshold）	自動アプリケーション バイパスのしきい値(ミリ秒)。

上記の設定は、いずれも [詳細設定(Advanced)] セクションを使用して編集できます。詳細については、次の各項を参照してください。

- 自動アプリケーション バイパス(3-3 ページ)
- 詳細なデバイス設定の編集(3-4 ページ)

自動アプリケーション バイパス

ライセンス:任意(Any)

自動アプリケーション バイパス(AAB)機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AAB により、その障害発生から 10 分以内に Snort が再起動され、トラブルシューティング データが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

このオプションが選択されている場合は、バイパスしきい値を変更できます。デフォルト設定は 3000 ミリ秒(ms)です。有効な範囲は 250 ms ～ 60,000 ms です。

(注) AAB がアクティブ化されるのは、単一パケットに過剰な処理時間がかかっている場合のみです。AAB がアクティブになると、システムはすべての Snort プロセスをキルします。

自動アプリケーション バイパスを有効にしてバイパスしきい値を設定する方法の詳細については、詳細なデバイス設定の編集(3-4 ページ)を参照してください。

詳細なデバイス設定の編集

[デバイス(Devices)] タブの [詳細設定(Advanced)] セクションを使用して、自動アプリケーション バイパスを変更できます。

詳細なデバイス設定を変更するには、以下を行います。

手順 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [デバイス管理(Device Management)] > [デバイス(Device)] の順に選択します。

[デバイス(Device)] ページが表示されます。

手順 2　[詳細設定(Advanced)] セクションの横にある編集アイコン( )をクリックします。

[詳細設定(Advanced)] ポップアップ ウィンドウが表示されます。

手順 3　ネットワークがレイテンシの影響を受けやすい場合は、必要に応じて、[自動アプリケーション バイパス(Automatic Application Bypass)] を選択します。自動アプリケーション バイパスは、インライン展開でとりわけ役立ちます。詳細については、自動アプリケーション バイパス(3-3 ページ)を参照してください。

手順 4　[自動アプリケーション バイパス(Automatic Application Bypass)] オプションを選択すると、[バイパスしきい値(Bypass Threshold)] にバイパスしきい値(ミリ秒)を入力できるようになります。デフォルト設定は 3000 ms です。有効な範囲は 250 ms ～ 60,000 ms です。

手順 5　[保存(Save)] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイス設定への変更の適用(3-5 ページ)を参照してください)。

ASA FirePOWER モジュール インターフェイスの管理

ライセンス: Control、Protection

ASA FirePOWER インターフェイスを編集する際に、ASA FirePOWER モジュール から設定できるのは、インターフェイスのセキュリティ ゾーンのみです。詳細については、セキュリティ ゾーンの操作(2-37 ページ)を参照してください。

ASDM および CLI を使用してインターフェイスを設定します。

ASA FirePOWER インターフェイスを編集するには、以下を行います。

手順 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [デバイス管理(Device Management)] > [インターフェイス(Interfaces)] の順に選択します。

[インターフェイス(Interfaces)] ページが表示されます。

手順 2　編集するインターフェイスの横にある編集アイコン( )をクリックします。

[インターフェイスの編集(Edit Interface)] ポップアップ ウィンドウが表示されます。

手順 3　[セキュリティ ゾーン(Security Zone)] ドロップダウンリストから、既存のセキュリティ ゾーンを選択するか、または [新規(New)] を選択して、新しいセキュリティ ゾーンを追加します。

手順 4　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

セキュリティ ゾーンが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用（3-5 ページ）を参照してください）。

デバイス設定への変更の適用

ライセンス：任意（Any）

デバイスの ASA FirePOWER 設定に変更を加えた後、モジュール全体に変更を反映するには、それらの変更を適用する必要があります。デバイスが変更適用前の状態でなければ、このオプションは無効になります。

インターフェイスを編集してデバイス ポリシーを再適用すると、編集したインターフェイス インスタンスだけでなく、デバイス上のすべてのインターフェイス インスタンスで Snort が再起動することに注意してください。

変更をデバイスに適用するには、以下を行います。

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] または [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] の順に選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　[ASA FirePOWER 変更の適用（Apply ASA FirePOWER Changes）] をクリックします。

手順 3　プロンプトが出されたら、[適用（Apply）] をクリックします。

デバイスの変更が適用されます。

ヒント　必要に応じて、[デバイス変更の適用（Apply Device Changes）] ダイアログ ボックスで [変更の表示（View Changes）] をクリックします。新しいウィンドウに [デバイス管理のレビジョン比較レポート（Device Management Revision Comparison Report）] ページが表示されます。詳細については、デバイス管理のリビジョン比較レポートの使用（3-6 ページ）を参照してください。

手順 4　[OK] をクリックします。

[デバイス管理（Device Management）] ページに戻ります。

デバイス管理のリビジョン比較レポートの使用

ライセンス:任意（Any）

デバイス管理の比較レポートを使用して、変更を確認してから、アプライアンスに適用できます。このレポートには、現在のアプライアンスの設定と、変更適用後のアプライアンスの設定との間の差異がすべて表示されます。これにより、設定の潜在的なエラーを検出することができます。

変更適用前と適用後のアプライアンスを比較するには、以下を行います。

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] または [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] の順に選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　[変更を適用（Apply Changes）] をクリックします。

[デバイス変更の適用（Apply Device Changes）] ポップアップ ウィンドウが表示されます。アプライアンスが変更適用前の状態でなければ、[変更を適用（Apply Changes）] ボタンは無効のままになります。

手順 3　[変更の表示（View Changes）] をクリックします。

新しいウィンドウに [デバイス管理のレビジョン比較レポート（Device Management Revision Comparison Report）] ページが表示されます。

手順 4　[前へ（Previous）] と [次へ（Next）] をクリックして、現在のアプライアンスの設定と変更適用後のアプライアンスの設定との間のすべての差異を確認します。

手順 5　必要に応じて、レポートの PDF バージョンを生成するには、[比較レポート（Comparison Report）] をクリックします。

リモート管理の設定

ライセンス:任意（Any）

ある FirePOWER システム アプライアンスと別のアプライアンスを相互に管理できるようにするには、その前に、2 つのアプライアンスの間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイ アベイラビリティ ピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

管理対象のアプライアンス、つまり Firepower Management Center で管理するデバイス上には、リモート管理を設定する必要があります。リモート管理を設定した後、管理側アプライアンスの Web インターフェイスを使用して、管理対象アプライアンスを展開環境に追加できます。

（注）　リモート管理を確立して、Firepower Management Center に Cisco ASA with FirePOWER Services を登録した後、ASDM の代わりに Firepower Management Center から ASA FirePOWER モジュール を管理する必要があります。アプライアンスを Firepower Management Center に登録すると、ASDM コンソールで Cisco ASA with FirePOWER Services をリモートから管理することは**できません**。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。通信を許可するために、FirePOWER システムでは 3 つの基準を使用します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー
- FirePOWER システムが NAT 環境で通信を確立するために利用できる、オプションの一意の英数字による NAT ID

  NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。

管理対象デバイスを Firepower Management Center に登録すると、ユーザが選択したアクセス コントロール ポリシーがデバイスに適用されます。ただし、選択したアクセス コントロール ポリシーで使用される機能に必要なライセンスがデバイスで有効になっていなければ、アクセス コントロール ポリシーの適用は失敗します。

ローカル アプライアンスのリモート管理を設定するには、以下を行います。

アクセス: 管理

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [リモート管理（Remote Management）] を選択します。

[リモート管理（Remote Management）] ページが表示されます。

手順 2　[マネージャの追加（Add Manager）] をクリックします。

[リモート管理の追加（Add Remote Management）] ページが表示されます。

手順 3　[管理ホスト（Management Host）] に、このアプライアンスを管理するために使用するアプライアンスの IP アドレスまたはホスト名を入力します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、FirePOWER システム は後で指定される NAT ID を使用して、管理対象 ASA FirePOWER モジュール インターフェイス上のリモート マネージャを識別します。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

手順 4　[登録キー（Registration Key）] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

手順 5　NAT 環境の場合は、[固有 NAT ID（Unique NAT ID）] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による**一意**の NAT ID を入力します。

手順 6　[保存（Save）] をクリックします。

アプライアンスが相互に通信できることを確認すると、ステータスとして [登録保留（Pending Registration）] が表示されます。

手順 7　管理側アプライアンスの Web ユーザ インターフェイスを使用して、このアプライアンスを展開環境に追加します。

（注）　NAT を使用する一部のハイ アベイラビリティ展開では、デバイスのリモート管理を有効にする際に、セカンダリ Firepower Management Center をマネージャとして追加しなければならない場合もあります。詳細については、サポートにお問い合わせください。

リモート管理の編集

ライセンス：任意（Any）

管理側アプライアンスのホスト名または IP アドレスを編集するには、以下の手順を使用します。また、管理側アプライアンスの表示名を変更することもできます。表示名は、FirePOWER システムのコンテキスト内でのみ使用されます。ホスト名をアプライアンスの表示名として使用することもできますが、別の表示名を入力してもホスト名は変更されません。

リモート管理を編集するには、以下を行います。

アクセス：Admin

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] > [登録（Registration）] の順に選択します。

[リモート管理（Remote Management）] ページが表示されます。

手順 2　リモート管理設定を編集するマネージャの横にある編集アイコン（）をクリックします。

[リモート管理の編集（Edit Remote Management）] ページが表示されます。

手順 3　[名前（Name）] フィールドで、管理側アプライアンスの表示名を変更します。

手順 4　[ホスト（Host）] フィールドで、管理側アプライアンスの IP アドレスまたはホスト名を変更します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

手順 5　[保存（Save）] をクリックします。

変更が保存されます。

eStreamer サーバ上での eStreamer 設定

ライセンス：FireSIGHT + Protection

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。

eStreamer イベント タイプの設定

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

管理対象デバイスまたは Firepower Management Center のいずれかで使用可能なイベント タイプは、以下のとおりです。

- 侵入イベント
- 侵入イベント パケット データ
- 侵入イベント追加データ

eStreamer によって送信されるイベントのタイプを設定する方法:

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] > [登録（Registration）] の順に選択します。

[登録（Registration）] ページが表示されます。

手順 2　[eStreamer] タブを選択します。

[eStreamer] ページが表示されます。

手順 3　[eStreamer イベント構成（eStreamer Event Configuration）] の下で、eStreamer から要求元のクライアントに転送するイベントのタイプの横にあるチェック ボックスをオンにします。

管理対象デバイスまたは Firepower Management Center で、次のいずれかまたはすべてを選択できます。

- [侵入イベント（Intrusion Events）]：侵入イベントを送信します。
- [侵入イベント パケット データ（Intrusion Event Packet Data）]：侵入イベントに関連付けられたパケットを送信します。
- [侵入イベント追加データ（Intrusion Event Extra Data）]：HTTP プロキシまたはロード バランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データを送信します。

（注）　これは、eStreamer サーバが送信できるイベントを制御することに注意してください。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、『*FirePOWER システム eStreamer Integration Guide*』を参照してください。

手順 4　[保存（Save）] をクリックします。

設定が保存され、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

eStreamer クライアントの認証の追加

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。

eStreamer クライアントを追加する方法:

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] > [登録（Registration）] の順に選択します。

[登録（Registration）] ページが表示されます。

手順 2　[eStreamer] タブを選択します。

[eStreamer] ページが表示されます。

手順 3　[クライアントの作成（Create Client）] をクリックします。

[クライアントの作成（Create Client）] ページが表示されます。

手順 4　[ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注）　ホスト名を使用する場合、eStreamer サーバはホストを IP アドレスに解決できる**必要**があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。

手順 5　証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

手順 6　[保存（Save）] をクリックします。

これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [ホスト名（Hostname）] の下に表示された状態で、[eStreamer] ページが再表示されます。

手順 7　クライアントのホスト名の横にあるダウンロード アイコン（ ）をクリックして、証明書ファイルをダウンロードします。

手順 8　SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

これで、クライアントは eStreamer に接続できるようになりました。eStreamer サービスを再起動する必要はありません。

ヒント　クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（ ）をクリックします。eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。