



デバイスの管理の基本

次のトピックでは、Firepower システムでデバイスを管理する方法について説明します。

- [\[デバイス管理 \(Device Management\) \] ページ \(1 ページ\)](#)
- [リモート管理の設定 \(3 ページ\)](#)
- [Firepower Management Center へのデバイスの追加 \(4 ページ\)](#)
- [Firepower Management Center からのデバイスの削除 \(6 ページ\)](#)
- [デバイス コンフィギュレーションの設定 \(7 ページ\)](#)
- [インターフェイス テーブル ビュー \(18 ページ\)](#)
- [デバイス グループ管理 \(23 ページ\)](#)
- [Firepower 2100 シリーズの SNMP の設定 \(25 ページ\)](#)

[デバイス管理 (Device Management)] ページ

[デバイス管理 (Device Management)] ページには、登録されたデバイス、7000 および 8000 シリーズデバイスのハイアベイラビリティ ペア、およびデバイス グループを管理するために使用できる、一連の情報とオプションが表示されます。このページには、現在 Firepower Management Center に登録されているすべてのデバイスの一覧が表示されます。

このページには、Firepower Management Center によって管理されている破損したデバイスの数も表示されます。ドリルダウンして、破損したデバイスの名前や IP アドレスを特定することができます。

[表示方法 (View by)] ドロップダウンリストを使用すると、グループ、ライセンス、モデル、またはアクセス コントロール ポリシーのいずれかのカテゴリでデバイス一覧をソートして表示できます。マルチドメイン導入では、ドメイン (その導入のデフォルトの表示カテゴリ) を基準にソートして表示することもできます。デバイスはリーフドメインに属している必要があります。

ヘルス モニタリング ステータスごとや、展開ステータスごとにデバイスを表示することもできます。

デバイス カテゴリに属するデバイスの一覧は、展開または縮小表示できます。デフォルトでは、デバイス一覧が展開されます。

デバイス一覧の詳細については、以下の表を参照してください。

表 1: [デバイス一覧 (Device List)] のフィールド

フィールド	説明
[名前 (Name)]	Firepower Management Center でデバイスに使用されている表示名。名前の左側にあるステータスアイコンは、その名前の現在のヘルスステータスを示します。
グループ	管理対象デバイスを割り当てたグループ。
モデル	管理対象デバイスのモデル。
バージョン (Version)	管理対象デバイス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。
ライセンス	管理対象デバイスで有効なライセンス。
アクセスコントロールポリシー (Access Control Policy)	現在導入されているアクセスコントロールポリシーへのリンク。システムがアクセスコントロールポリシーを古いものとして識別すると、そのリンクの横に警告アイコン (ⓘ) が表示されます。

関連トピック

- [Firepower の機能ライセンスについて](#)
- [ヘルス モニタリングについて](#)
- [アクセスコントロールポリシーの管理](#)

管理対象デバイスのフィルタリング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

Firepower Management Center が大量のデバイスを管理する場合、[デバイス管理 (Device Management)] ページの結果を絞り込むことで特定のデバイスを見つけやすくなります。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ2 デバイスのリストを絞り込むには、[デバイス名 (DeviceName)][デバイス検索 (SearchDevice)] フィールドにデバイス名、ホスト名または IP アドレスの全体または一部を入力します。

ステップ3 フィルタをクリアするには、[デバイス検索 (Search Device)] フィールドをクリアします。

関連トピック

[Firepower の機能ライセンスについて](#)

[ヘルス モニタリングについて](#)

[アクセス コントロール ポリシーの管理](#)

リモート管理の設定

Firepower System デバイスを管理できるようにするには、デバイスと Firepower Management Center との間に双方向の 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。



(注) この章では、FMCにデバイスを登録する前にローカル Web インターフェイスを使用して、7000 または 8000 シリーズ デバイスのリモート管理の設定方法について説明します。他のモデルのリモート管理の設定の詳細については、適切なクイックスタートガイドを参照してください。

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。Firepower System では3つの基準を使用して、通信を許可します。

- 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 System 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。

Firepower Management Center へのデバイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Network Admin

Firepower Management Center に 1 つのデバイスを追加するには、ここに示す手順を実行します。冗長性やパフォーマンスのためにデバイスをリンクする場合、次の点を念頭に置いて、この手順を実行する必要があります。

- 8000 シリーズ スタック：この手順を使用して各デバイスを Firepower Management Center に追加した後、スタックを確立します ([デバイス スタックの確立](#)を参照)。
- 7000 および 8000 シリーズ ハイ アベイラビリティ：この手順を使用して各デバイスを Firepower Management Center に追加した後、高可用性を確立します ([デバイスのハイ アベイラビリティの確立](#)を参照)。ハイアベイラビリティスタックの場合、デバイスをスタックしてから、スタック間のハイ アベイラビリティを確立します。
- Firepower Threat Defense ハイアベイラビリティ：この手順を使用して各デバイスを Firepower Management Center に追加した後、高可用性を確立します ([Firepower Threat Defense ハイアベイラビリティ ペアの追加](#)を参照)。
- Firepower Threat Defense クラスタ：クラスタ ユニットが FXOS に正常に形成されたクラスタであることを確認し、次の手順を使用して各ユニットを別個の管理対象デバイスとして Firepower Management Center に追加します。最後に、Firepower Management Center でユニットをクラスタ化します。詳細については、[Management Center へのクラスタの追加](#)を参照してください。



(注) Firepower Management Center ハイアベイラビリティを確立したか、または確立する予定がある場合、デバイスをアクティブな (またはアクティブにする予定の) Firepower Management Center にのみ追加します。ハイアベイラビリティを確立すると、アクティブ Firepower Management Center に登録されたデバイスが自動的にスタンバイに登録されます。

始める前に

- デバイスを Firepower Management Center の管理対象として設定します。7000 および 8000 シリーズデバイスについては、[管理対象デバイス上のリモート管理の設定](#)を参照してください。他のモデルのリモート管理設定の詳細については、該当するクイックスタートガイドを参照してください。
- IPv4 を使用して登録した Firepower Management Center とデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** [追加 (Add)] ドロップダウンメニューから、[デバイスの追加 (Add Device)] を選択します。
- ステップ 3** [ホスト (Host)] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。
- デバイスのホスト名は、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。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。
- NAT 環境では、Firepower Management Center の管理対象としてデバイスを設定するときに Firepower Management Center の IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要がない場合があります。詳細については、[NAT 環境](#)を参照してください。
- ステップ 4** [表示名 (Display Name)] フィールドに、Firepower Management Center でのデバイスの表示名を入力します。
- ステップ 5** [登録キー (Registration Key)] フィールドに、Firepower Management Center の管理対象としてデバイスを設定したときに使用したのと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。
- ステップ 6** マルチドメイン展開では、現在のドメインに関係なく、デバイスをリーフドメインに割り当てます。
- 現在のドメインがリーフドメインである場合、デバイスは自動的に現在のドメインに追加されます。現在のドメインがリーフドメインでない場合、登録後、デバイスを設定するために、リーフドメインに切り替える必要があります。
- ステップ 7** 必要に応じて、デバイスをデバイスグループに追加します。
- ステップ 8** 登録後すぐに、デバイスに展開する最初の [アクセスコントロールポリシー (Access Control Policy)] を選択するか、新しいポリシーを作成します。
- デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。この障害の原因を解決した後、デバイスに手作業で設定を行います。
- ステップ 9** デバイスに適用するライセンスを選択します。
- 従来型のデバイスでは、次の点に注意してください。
- コントロール、マルウェア、URL フィルタリングライセンスには、保護ライセンスが必要です。
 - VPN ライセンスでは、7000 または 8000 シリーズ デバイスを必要とします。

- コントロール ライセンスは、NGIPSv と ASA FirePOWER デバイスでサポートされていますが、8000 シリーズ Fastpath ルール、スイッチング、ルーティング、スタック、デバイスのハイ アベイラビリティを設定することはできません。

ステップ 10 デバイスの設定時に、NAT ID を使用した場合、[詳細 (Advanced)] セクションを展開し、[一意の NAT ID (Unique NAT ID)] フィールドに同じ NAT ID を入力します。

ステップ 11 [パケットの転送 (Transfer Packets)] チェックボックスをオンにし、デバイスで Firepower Management Center にパケットを転送することを許可します。

このオプションは、デフォルトで有効です。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Firepower Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Firepower Management Center に送信され、パケットデータは送信されません。

ステップ 12 [登録 (Register)] をクリックします。

Firepower Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。

関連トピック

[基本的なアクセス コントロール ポリシーの作成](#)

Firepower Management Center からのデバイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Network Admin

デバイスを管理する必要がなくなった場合、Firepower Management Center からそのデバイスを削除できます。デバイスを削除すると、以下のようになります。

- Firepower Management Center とそのデバイスとの間のすべての通信が切断されます。
- [デバイス管理 (Device Management)] ページからデバイスが削除されます。
- プラットフォーム設定ポリシーで、NTP を介して Firepower Management Center から時間を受信するようにデバイスが設定されている場合は、デバイスがローカル時間管理に戻されます。

デバイスを後方で管理するには、デバイスを Firepower Management Center に再度追加します。



- (注) デバイスを削除し、再び追加すると、Firepower Management Center Web インターフェイスによって、アクセス コントロール ポリシーを再適用するよう求められます。ただし、登録時に NAT と VPN ポリシーを再適用するオプションはありません。以前に適用された NAT または VPN 設定はすべて登録時に削除されるため、登録が完了した後に再適用する必要があります。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 削除するデバイスの横にある削除アイコン (🗑️) をクリックします。
- ステップ 3** デバイスを削除することを確認します。

デバイス コンフィギュレーションの設定

アプライアンス エディタの [デバイス (Device)] ページには、詳細なデバイス設定および情報が表示されます。また、デバイス設定の一部 (ライセンスの有効化と無効化、デバイスのシャットダウンと再起動、管理の変更、詳細オプションの設定など) を変更することもできます。

一般的なデバイスの設定

[デバイス (Device)] タブの [全般 (General)] セクションには、以下の表に記載された設定を表示します。

表 2: [全般 (General)] セクション テーブルのフィールド

フィールド	説明
[名前 (Name)]	Firepower Management Center でのデバイスの表示名。
パケット転送 (Transfer Packets)	管理対象デバイスがイベントを含むパケットデータを Firepower Management Center に送信するかどうか。
[モード (Mode)]	デバイスの管理インターフェイスのモード: [ルーテッド (routed)] または [トランスパレント (transparent)]。
展開を強制 (Force Deploy)	デバイスのすべてのポリシーおよびデバイス設定の更新を強制的に展開します。

デバイス ライセンスの設定

[デバイス (Device)]タブの[ライセンス (License)]セクションでは、そのデバイスに対して有効になっているライセンスが表示されます。

関連トピック

[Firepower の機能ライセンスについて](#)

デバイス システムの設定

[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:[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	管理対象デバイスのモデル名と番号。
シリアル (Serial)	管理対象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)	管理対象デバイス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	管理対象デバイスに現在展開されているプラットフォーム設定ポリシーへのリンク。
インベントリ	<p>関連する Firepower 2100 デバイスのインベントリ詳細情報へのリンク。[インベントリ詳細 (Inventory Details)]ウィンドウには、FXOS プラットフォームの REST API から取得された次の情報が表示されます。</p> <ul style="list-style-type: none"> • ファン • メモリ • CPU • 電源モジュール • [ストレージ (Storage)] • ネットワーク モジュール <p>このフィールドは、Firepower 2100 デバイスの Firepower Management Center のみで表示されます。</p>

デバイスをシャットダウンまたは再起動することもできます。

デバイスヘルスの設定

[デバイス (Device)] タブの [ヘルス (Health)] セクションには、以下の表に記載された情報を表示します。

表 4:[ヘルス (Health)]セクションテーブルのフィールド

フィールド	説明
ステータス (Status)	デバイスの現在のヘルス ステータスを表すアイコン。アイコンをクリックすると、アプライアンスのヘルス モニタが表示されます。
ポリシー	現在デバイスで展開されている、読み取り専用バージョンの正常性ポリシーへのリンク。
ブラックリスト	[ヘルス ブラックリスト (Health Blacklist)] ページへのリンク。このページでは、ヘルス ブラックリスト モジュールを有効または無効に設定できます。

関連トピック

[アプライアンスヘルスモニタの表示](#)

[正常性ポリシーの編集](#)

[正常性ポリシーモジュールのブラックリスト登録](#)

デバイス管理設定

[デバイス (Device)] タブの [管理 (Management)] セクションには、以下の表に記載されたフィールドを表示します。

表 5:[管理 (Management)]セクションテーブルのフィールド

フィールド	説明
ホスト	デバイスの IP アドレスまたはホスト名。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（つまり、ホスト名）です。

フィールド	説明
ステータス	Firepower Management Center と管理対象デバイス間の通信チャネルのステータスを示すアイコン。ステータス アイコンにポインタを置くと、Firepower Management Center が最後にデバイスにアクセスした時間を表示することができます。

デバイスの詳細設定

[デバイス (Device)] タブの [詳細設定 (Advanced)] セクションには、以下で説明する詳細設定のテーブルが表示されます。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。

表 6: [詳細設定 (Advanced)] セクションのテーブルのフィールド

フィールド	説明	サポートされるデバイス
アプリケーション バイパス (Application Bypass)	デバイスでの自動アプリケーション バイパスの状態。	7000 & 8000 シリーズ、NGIPSv、ASA FirePOWER、Firepower Threat Defense
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)。	7000 & 8000 シリーズ、NGIPSv、ASA FirePOWER、Firepower Threat Defense
ローカル ルータ トラフィック を検査する (Inspect Local Router Traffic)	デバイスで、ルーテッド インターフェイスで受信した自己宛先とするトラフィック (ICMP、DHCP、および OSPF トラフィックなど) を検査するかどうかを示します。	7000 & 8000 シリーズ
高速パス ルール (Fast-Path Rules)	デバイスで作成されている 8000 シリーズ 高速パス ルールの数。	8000 シリーズ

デバイス情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Network Admin

マルチドメイン展開では、先祖ドメインは、子孫ドメイン内のすべてのデバイスに関する情報を表示できます。デバイスを編集するリーフドメインに位置している必要があります。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、先祖ドメインに位置している場合、表示アイコン (🔍) をクリックすると、読み取り専用モードで子孫ドメインのデバイスを表示できます。

ステップ 3 [デバイス (Device)] タブをクリックします。

ステップ 4 次の情報が表示されます。

- [全般 (General)] : デバイスの一般設定を表示します (一般的なデバイスの設定 (7 ページ) を参照)。
- [ライセンス (License)] : デバイスのライセンス情報を表示します (デバイスライセンスの設定 (8 ページ) を参照)。
- [システム (System)] : デバイスのシステム情報を表示します (デバイスシステムの設定 (8 ページ) を参照)。
- [ヘルス (Health)] : デバイスの現在のヘルス ステータスに関する情報を表示します (デバイスヘルスの設定 (9 ページ) を参照)。
- [管理 (Management)] : Firepower Management Center とデバイス間の通信チャンネルに関する情報を表示します (デバイス管理設定 (9 ページ) を参照)。
- [詳細 (Advanced)] : 高度な機能設定に関する情報を表示します (デバイスの詳細設定 (10 ページ) を参照)。

デバイス管理設定の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin



(注) 場合によっては、(デバイスの LCD パネルまたは CLI などを使用して) 別の方法でデバイスのホスト名や IP アドレスを編集する場合は、次の手順を実行して、管理用の Firepower Management Center でホスト名や IP アドレスを手動で更新する必要があります。

手順

ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ2 管理オプションを変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ3 [デバイス (Device)] タブをクリックします。

ヒント スタック構成のデバイスの場合、アプライアンスエディタの [デバイス (Devices)] ページで、個々のデバイスの管理オプションを変更します。

ステップ4 次の操作を実行できます。

- リモート管理の無効化：[管理 (Management)] セクションのスライダをクリックして、デバイスの管理を有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除されません。デバイスを管理する必要がなくなった場合は、[Firepower Management Center からのデバイスの削除 \(6 ページ\)](#) を参照してください。
- 管理ホストの編集：[管理 (Management)] セクションの編集アイコン (✎) をクリックし、[ホスト (Host)] フィールドで名前または IP アドレスを変更し、[保存 (Save)] をクリックします。この設定を使用して、管理ホスト名を指定したり、仮想 IP アドレスを再生成することができます。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

一般的なデバイス設定の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

手順

ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ2 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス (Device)] をクリックします。

ステップ 4 [一般 (General)] セクションで、編集アイコン (✎) をクリックします。

ステップ 5 [名前 (Name)] に、管理対象デバイスの名前を入力します。

ヒント スタック構成のデバイスの場合、アプライアンスエディタの[スタック (Stack)] ページで、スタックでデバイスに割り当てられている名前を編集します。アプライアンスエディタの [デバイス (Devices)] ページでは、個々のデバイスに割り当てられているデバイス名を編集できます。

ステップ 6 [パケットの転送 (Transfer Packets)] 設定を変更します。

- パケットデータをイベントと一緒に Firepower Management Center 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。
- 管理対象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。

ステップ 7 [強制展開 (Force Deploy)] をクリックし、デバイスに現在のポリシーとデバイス設定の展開を強制します。

ステップ 8 [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

デバイス ライセンスの有効化と無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

Firepower Management Center で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 ライセンスを有効または無効にするデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス (Device)] タブをクリックします。

ヒント スタック構成のデバイスの場合、アプライアンスエディタの[スタック (Stack)] ページで、スタックに対してライセンスを有効または無効にします。

ステップ 4 [ライセンス (License)] セクションで、編集アイコン (✎) をクリックします。

ステップ 5 管理対象デバイスに対して有効または無効にするライセンスの横にあるチェックボックスをオンまたはオフにします。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。 [設定変更の展開](#) を参照してください。

関連トピック

[Firepower の機能ライセンスについて](#)

詳細なデバイス設定の編集

アプリケーションバイパス、ローカルルータトラフィックのインスペクション、および高速パスのルールを設定できます。

自動アプリケーションバイパスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin Network Admin

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。

一般に、遅延しきい値を超えた後は、高速パスパケットに対して侵入ポリシーの [ルール遅延しきい値 (Rule Latency Thresholding)] を使用します。 [ルール遅延しきい値 (Rule Latency

Thresholding)]により、エンジンがシャットダウンされたり、しきい値データが生成されることはありません。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。



注意 単一パケットに過剰な処理時間がかかっている場合、AAB がアクティブになります。AAB のアクティブ化は、いくつかのパケットのインスペクションを一時的に中断する Snort プロセスを部分的に再起動します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作](#)を参照してください。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 高度なデバイス設定を編集するデバイスの横にある編集アイコン (✎) をクリックします。
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [デバイス (Device)] タブ (またはスタック構成のデバイスの場合は [スタック (Stack)] タブ) をクリックし、[詳細 (Advanced)] セクションの編集アイコン (✎) をクリックします。
- ステップ 4** [自動アプリケーションバイパス (Automatic Application Bypass)] をオンにします。
- ステップ 5** [バイパスしきい値 (Bypass Threshold)] に 250 ~ 60,000 ミリ秒を入力します。デフォルト設定は 3000 ミリ秒 (ms) です。
- ステップ 6** [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

ローカルルータ トラフィックの検査

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ローカル内トラフィックがレイヤ3展開のモニターールと一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックの検査を確認するには、[ローカルルータ トラフィックの検査 (Inspect Local Router Traffic)] を有効にします。

手順

- ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ2 高度なデバイス設定を編集するデバイスの横にある編集アイコン (✎) をクリックします。
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ3 [デバイス (Devices)] タブ (スタック構成のデバイスの場合は [スタック (Stack)] タブ) をクリックして、[詳細 (Advanced)] セクションの編集アイコン (✎) をクリックします。
- ステップ4 7000 または 8000 シリーズ デバイスがルータとして展開されている場合は、[ローカルルータトラフィックの検査] をオンにして、例外トラフィックを検査します。
- ステップ5 [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。 [設定変更の展開](#) を参照してください。

高速パス ルールの設定 (8000 シリーズ)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	8000 シリーズ	リーフのみ	Admin/Network Admin

トラフィック処理の初期形式として、8000 シリーズ高速パス ルールでは、それ以上のインスペクションやロギングを行わずに 8000 シリーズ デバイスを介してトラフィックを直接送信できます。(パッシブ展開では、8000 シリーズ高速パス ルールは単に分析を停止します)。各 8000 シリーズ高速パス ルールは、特定のセキュリティゾーンまたはインラインインターフェイスセットに適用されます。8000 シリーズ高速パス ルールはハードウェアレベルで機能するため、高速パス トラフィックには、次の単純な外部ヘッダーの基準のみを使用できます。



- 発信側および応答側の IP アドレスまたはアドレス ブロック
- プロトコル、および TCP と UDP の場合は、発信側および応答側のポート
- VLAN ID (Admin. VLAN ID)

デフォルトでは、8000 シリーズ高速パス ルールは指定した発信側から指定した応答側への接続に影響します。ルールの基準を満たすすべての接続を高速パス処理するには、どちらのホストが発信側か応答側かに関係なく、ルールを双方向にすることができます。



(注) 同様の機能を実行しますが、8000 シリーズ高速パス ルールはプレフィルタ ポリシーで設定する高速パス トンネルやプレフィルタ ルールに関連しません。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 ルールを設定する 8000 シリーズデバイスの横にある編集アイコン () をクリックします。
マルチドメイン展開では、リードドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [デバイス (Device)] タブ (またはスタック構成のデバイスの場合は [スタック (Stack)] タブ) をクリックし、[詳細 (Advanced)] セクションの編集アイコン () をクリックします。
- ステップ 4 [新しい IPv4 ルール (New IPv4 Rule)] または [新しい IPv6 ルール (New IPv6 Rule)] をクリックします。
- ステップ 5 [ドメイン (Domain)] ドロップダウン リストから、インラインセットまたはパッシブセキュリティ ゾーンを選択します。
- ステップ 6 高速パス処理するトラフィックを設定します。トラフィックは高速パス処理のためのすべての条件を満たしている必要があります。
 - [発信側 (Initiator)] および [応答側 (Responder)] (必須) : 発信側および応答側の IP アドレスまたはアドレス ブロックを入力します。
 - [プロトコル (Protocol)] : プロトコルを選択するか、[すべて (All)] を選択します。
 - [発信側ポート (Initiator Port)] および [応答側ポート (Responder Port)] : TCP および UDP トラフィックの場合は、発信側ポートと応答側ポートを入力します。フィールドを空白のままにするか、**Any** と入力して、すべての TCP または UDP トラフィックに一致するようにします。ポートのカンマ区切りリストを入力できますが、ポート範囲を入力することはできません。
 - [VLAN] : VLAN ID を入力します。フィールドを空白のままにするか、**Any** と入力して、VLAN タグに関係なくすべてのトラフィックに一致するようにします。
- ステップ 7 (任意) ルールを [双方向 (Bidirectional)] にします。
- ステップ 8 [保存 (Save)] をクリックしてから、もう一度 [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

システム シャットダウンの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (ASA FirePOWER を除く)	リーフのみ	Admin/Network Admin



(注) Firepower システムのユーザインターフェイスでは、ASA FirePOWER のシャットダウンまたは再起動はできません。それぞれのデバイスをシャットダウンする方法の詳細については、ASA の資料を参照してください。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス (Device)] タブをクリックします。

ヒント スタックに含まれるデバイスの場合、アプライアンスエディタの [デバイス (Devices)] ページで、個々のデバイスをシャットダウンまたは再起動します。

ステップ 4 デバイスをシャットダウンするには、[システム (System)] セクションでデバイスのシャットダウンアイコン (●) をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 デバイスを再起動するには、デバイスの再起動アイコン (🔄) をクリックします。

ステップ 7 プロンプトが表示されたら、デバイスを再起動することを確認します。

インターフェイス テーブル ビュー

ハードウェア ビューの下にあるインターフェイス テーブル ビューには、デバイスで使用可能なすべてのインターフェイスが一覧表示されます。テーブル内のナビゲーションツリーを展開すると、設定されているすべてのインターフェイスを表示できます。インターフェイスの横にある矢印アイコンをクリックして、インターフェイスを縮小または展開することで、サブコン

ポートの非表示/表示を切り替えることができます。このインターフェイステーブルビューには、各インターフェイスに関する以下の要約情報が表示されます。

従来のデバイスのインターフェイス

[MAC アドレス (MAC Address)] 列と [IP アドレス (IP Address)] 列が表示されるのは、8000 シリーズ デバイスのみです。詳細については、次の表を参照してください。

表 7: 従来のデバイスのインターフェイス テーブル ビューのフィールド

フィールド	説明
[名前 (Name)]	

フィールド	説明
	<p>各インターフェイス タイプは、タイプとリンク ステート（該当する場合）を示す固有のアイコンによって表されます。名前またはアイコンの上にマウス ポインタを移動すると、インターフェイス タイプ、速度、デュプレックス モード（該当する場合）がツールチップに表示されます。インターフェイス アイコンについては、インターフェイス アイコンを参照してください。</p> <p>アイコンでは、インターフェイスの現在のリンク状態を示す表示方法が使用されています。次の3つの状態のいずれかが表示されます。</p> <ul style="list-style-type: none"> • エラー  • 障害  • 使用不可  <p>論理インターフェイスのリンク状態は、親物理インターフェイスのリンク状態と同じです。ASA FirePOWER モジュールには、リンク状態は表示されません。無効化されたインターフェイスは、半透明のアイコンで表されます。</p> <p>アイコンの右側に表示されるインターフェイス名は自動生成されます。ただし、ハイブリッドインターフェイスと ASA FirePOWER インターフェイスの名前はユーザが定義します。ASA FirePOWER インターフェイスについては、名前が付けられており、リンクを持つ有効なインターフェイスのみが表示されることに注意してください。</p> <p>物理インターフェイスでは、物理インターフェイスの名前が表示されます。論理インターフェイスでは、物理インターフェイスの名前と、割り当てられている VLAN タグが表示されます。</p> <p>ASA FirePOWER インターフェイスでは、複数のセキュリティ コンテキストがある場合は、セキュリティ コンテキストの名前とインターフェイスの名前が表示されます。セキュリティ コンテキストが1つしかない場合は、インター</p>

フィールド	説明
	フェイスの名前のみが表示されます。
セキュリティ ゾーン (Security Zone)	インターフェイスが割り当てられているセキュリティゾーン。セキュリティゾーンを追加または編集するには、編集アイコン (✎) をクリックします。
使用者 (Used by)	インターフェイスが割り当てられているインラインセット、仮想スイッチ、または仮想ルータ。ASA FirePOWER モジュールでは、[使用者 (Used by)] 列は表示されません。
MAC アドレス (MAC Address)	スイッチド機能およびルーテッド機能で有効にされているインターフェイスに対して表示される MAC アドレス。 NGIPSv デバイスの場合、表示された MAC アドレスにより、デバイス上に設定されたネットワーク アダプタと、[インターフェイス (Interfaces)] ページに表示されるインターフェイスを対応させることができます。ASA FirePOWER モジュールでは、MAC アドレスは表示されません。
IP アドレス	インターフェイスに割り当てられた IP アドレス。マウスのポインタを IP アドレスの上に重ねると、その IP アドレスがアクティブであるか非アクティブであるかを確認できます。非アクティブな IP アドレスはグレー表示されます。ASA FirePOWER モジュールでは、IP アドレスは表示されません。

Firepower Threat Defense のインターフェイス

表 8: Firepower Threat Defense のインターフェイス テーブル ビューのフィールド

フィールド	説明
インターフェイス (Interface)	インターフェイス ID。フェールオーバーリンクまたはクラスタ制御リンクのインターフェイスの場合、インターフェイス設定は表示専用です。
論理名 (Logical Name)	インターフェイスの構成名。

フィールド	説明
タイプ (Type)	インターフェイスのタイプ: [物理 (Physical)]、[サブインターフェイス (SubInterface)]、[EtherChannel]、[冗長 (Redundant)]、または [ブリッジグループ (BridgeGroup)] (トランスペアレント ファイアウォール モードのみ)。
インターフェイス オブジェクト (Interface Object)	インターフェイスが割り当てられているセキュリティゾーンまたはインターフェイスグループ。
MAC アドレス (MAC Address) (アクティブ/スタンバイ)	インターフェイスの MAC アドレス。ハイアベイラビリティの場合、アクティブな MAC アドレスとスタンバイ状態の MAC アドレスの両方が表示されます。
[IP アドレス (IP Address)]	インターフェイスに割り当てられている IP アドレス。括弧で示されるアドレス割り当てのタイプ: [静的 (Static)]、[DHCP]、または [PPPoE]。

デバイス グループ管理

Firepower Management Center でデバイスをグループ化すると、複数のデバイスへのポリシーの展開やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

マルチドメイン展開では、リーフドメイン内でのみデバイスグループを作成できます。Firepower Management Center をマルチテナンシー向けに設定すると既存のデバイスグループは削除されます。デバイスグループはリーフドメインレベルで再度追加できます。

デバイス グループの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

デバイスグループにより、複数デバイスへのポリシーの割り当てとインストール更新が簡単にできます。

スタック内または高可用性ペア内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除または高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 [追加 (Add)] ドロップダウンメニューから、[グループの追加 (Add Group)] を選択します。
- ステップ 3 名前を入力します。
- ステップ 4 [使用可能なデバイス (Available Devices)] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。
- ステップ 5 [追加 (Add)] をクリックして、選択したデバイスをデバイス グループに追加します。
- ステップ 6 [OK] をクリックして、デバイス グループを追加します。

デバイス グループの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

任意のデバイスグループに含まれる一連のデバイスを変更できます。アプライアンスは、現行のグループから削除してからでないと、新しいグループに追加できません。

アプライアンスを新しいグループに移動しても、そのアプライアンスのポリシーが、新しいグループにすでに割り当てられているポリシーに変更される訳ではありません。グループのポリシーを新しいデバイスに割り当てる必要があります。

スタック内またはデバイスのハイ アベイラビリティ ペア内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除または高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

マルチドメイン展開では、デバイスグループは、それらが作成されたドメイン内でのみ編集できます。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 編集するデバイス グループの横にある編集アイコン (✎) をクリックします。

- ステップ 3** 必要に応じて、[名前 (Name)] フィールドに、グループの新しい名前を入力します。
- ステップ 4** [使用可能なデバイス (Available Devices)] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。
- ステップ 5** [追加 (Add)] をクリックして、選択したデバイスをデバイス グループに追加します。
- ステップ 6** 必要に応じて、デバイスグループからデバイスを削除するには、削除するデバイスの横にある削除アイコン (🗑️) をクリックします。
- ステップ 7** [OK] をクリックして、デバイス グループに加えた変更を保存します。

Firepower 2100 シリーズの SNMP の設定

簡易ネットワーク管理プロトコル (SNMP) は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- **SNMP マネージャ** : SNMP を使用してネットワークデバイスのアクティビティを制御し、モニタリングするシステム
- **SNMP エージェント** : Firepower シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに報告する Firepower 2100 シャーシ内のソフトウェア コンポーネント。Firepower シャーシには、エージェントと一連の MIB が含まれています。SNMP エージェントを有効にし、マネージャとエージェント間のリレーションシップを作成するには、Firepower Management Center で SNMP を有効にし、設定します。
- **管理情報ベース (MIB)** : SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower 2100 シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。

SNMP を有効化し、Firepower 2100 用に SNMP プロパティを設定する



(注) この手順は Firepower 2100 シリーズ デバイスにのみ該当します。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

SNMP を有効化し、Firepower 2100 用に SNMP プロパティを設定する

ステップ 2 [SNMP] タブをクリックします。

ステップ 3 次のフィールドに入力します。

[名前 (Name)]	説明
[管理状態 (Admin State)] チェックボックス	SNMP を有効にするかまたは無効にするか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスを有効にします。
[ポート (Port)] フィールド	Firepower シャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。
[コミュニティ (Community)] フィールド	Firepower シャーシが SNMP ホストに送信するトラップメッセージに含まれるデフォルトの SNMP v1 または v2 コミュニティの名前、あるいは SNMP v3 のユーザ名。 1 ~ 32 文字の英数字文字列を入力します。@ (アットマーク)、\ (バックスラッシュ)、" (二重引用符)、? (疑問符) または空欄スペースは使用しないでください。デフォルトは public です。 [コミュニティ (Community)]フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [設定: はい (Set: Yes)] となることに注意してください。[コミュニティ (Community)]フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [設定: いいえ (Set: No)] となります。
[システム管理者名 (System Admin Name)] フィールド	SNMP の実装担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[ロケーション (Location)] フィールド	SNMP エージェント (サーバ) が動作するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

SNMP トラップおよびユーザを作成します。

Firepower 2100 用の SNMP トラップの作成



(注) この手順は Firepower 2100 シリーズ デバイスにのみ該当します。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 [SNMP] タブをクリックします。
- ステップ 3 [SNMP トラップ設定 (SNMP Traps Configuration)] 領域で、[追加 (Add)] をクリックします。
- ステップ 4 [SNMP トラップ設定 (SNMP Trap Configuration)] ダイアログボックスで、次のフィールドに値を入力します。

名前 (Name)]	説明
[ホスト名 (Host Name)] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[コミュニティ (Community)] フィールド	Firepower シャーシがトラップを SNMP ホストに送信するときに含める SNMP v1 または v2 のコミュニティ名または SNMP v3 のユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ~ 32 文字の英数字文字列を入力します。@ (アットマーク)、\ (バックスラッシュ)、" (二重引用符)、? (疑問符) または空欄スペースは使用しないでください。
[ポート (Port)] フィールド	Firepower シャーシがトラップのために SNMP ホストと通信するポート。 1 ~ 65535 の整数を入力します。
[バージョン (Version)] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 <ul style="list-style-type: none"> • V1 • V2 • V3
[タイプ (Type)] フィールド	バージョンとして [V2] または [V3] を選択した場合に、送信するトラップのタイプ。次のいずれかになります。 <ul style="list-style-type: none"> • トラップ • 情報

[名前 (Name)]	説明
[特権 (Privilege)]フィールド	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。 <ul style="list-style-type: none"> • [認証 (Auth)] : 認証あり、暗号化なし • [認証なし (Noauth)] : 認証なし、暗号化なし • [秘密 (Priv)] : 認証あり、暗号化あり

ステップ 5 [OK] をクリックして、[SNMP トラップ設定 (SNMP Trap Configuration)] ダイアログボックスを閉じます。

ステップ 6 [保存 (Save)] をクリックします。

Firepower 2100 用の SNMP ユーザの作成



(注) この手順は Firepower 2100 シリーズ デバイスにのみ該当します。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 [SNMP] タブをクリックします。

ステップ 3 [SNMP ユーザ設定 (SNMP Users Configuration)] 領域で、[追加 (Add)] をクリックします。

ステップ 4 [SNMP ユーザ設定 (SNMP User Configuration)] ダイアログボックスで、次のフィールドに値を入力します。

[名前 (Name)]	説明
[ユーザ名 (Username)] フィールド	SNMP ユーザに割り当てられるユーザ名。 32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_ (アンダースコア) 、. (ピリオド) 、@ (アットマーク) 、- (ハイフン) も指定できます。
[認証アルゴリズム タイプ (Auth Algorithm Type)] フィールド	許可タイプ : SHA 。
[AES-128 を使用 (Use AES-128)] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。

[名前 (Name)]	説明
[認証パスワード (Authentication Password)] フィールド	ユーザのパスワード。
[確認 (Confirm)] フィールド	確認のためのパスワードの再入力。
[暗号化パスワード (Encryption Password)] フィールド	ユーザのプライバシー パスワード。
[確認 (Confirm)] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 5 [OK] をクリックして、[SNMP ユーザ設定 (SNMP User Configuration)] ダイアログボックスを閉じます。

ステップ 6 [保存 (Save)] をクリックします。

