ポリシー管理

ここでは、Firepower Management Center でさまざまなポリシーを管理する方法について説明します。

ポリシーの導入

導入を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を導入する必要があります。導入のステータスは、メッセージ センターで確認できます。

導入を行うと、以下のコンポーネントが更新されます。

- デバイスとインターフェイスの設定
- デバイス関連ポリシー：NAT、VPN、QoS、プラットフォーム設定
- アクセス コントロールおよび関連するポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、プレフィルタ、SSL
- ネットワーク検出ポリシー
- 侵入ルールの更新
- これらの要素のいずれかに関連付けられている設定とオブジェクト

システムにポリシーを自動的に導入させるには、導入タスクをスケジュールするか、あるいは侵入ルールの更新をインポートする際に導入するようにシステムを設定します。特に、侵入ポリシーの更新によって侵入およびネットワーク分析に関するシステム定義の基本ポリシーを変更できるようにしている場合は、ポリシーの導入を自動化すると役立ちます。侵入ルール更新によって、アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細設定オプションのデフォルト値が変更されることもあります。

マルチドメイン展開では、ユーザアカウントが属するいずれのドメインにも変更を導入できます。

- 導入先を先祖ドメインに切り替えると、変更がすべてのサブドメインに同時に導入されます。
- 導入先をリーフ ドメインに切り替えると、変更はそのドメインだけに導入されます。

設定変更の展開に関する注意事項

インライン展開とパッシブ展開の比較

インライン設定をパッシブに展開されたデバイスに適用しないでください。またその逆も同様です。

展開時間とメモリの制限

展開に要する時間は、次のような複数の要因によって異なります（ただし、これに限られません）。

- デバイスに送信する設定。たとえば、ブロックするセキュリティ インテリジェンス エントリの数を大幅に増やすと、展開にかかる時間が長くなることがあります。
- デバイスのモデルとメモリ。低メモリ デバイスでは、展開にかかる時間が長くなることがあります。たとえば、FirePOWER 7010、7020、または 7030 デバイスへの展開に最大で 5 分かかることがあります。

デバイスの機能を超えないように注意してください。ターゲット デバイスでサポートされるルールまたはポリシーの最大数を超えると、システムが警告を表示します。最大数は多くの要因に依存し、メモリとデバイス上のプロセッサ数だけでなく、ポリシーとルールの複雑さにも依存します。ポリシーとルールの最適化の詳細については、ルールのパフォーマンスに関するガイドラインを参照してください。

展開中のトラフィック フローとインスペクションの中断

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。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。Snort® の再起動によるトラフィックの動作 （10 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定 （12 ページ）を参照してください。

Firepower Threat Defense デバイスでは、[展開（Deploy）] ダイアログの [インスペクションの中断（Inspect Interruption）] 列により、展開時にトラフィック フローまたはインスペクションが中断される可能性があることが警告されます。展開を続行、キャンセル、または延期できます。詳細については、Firepower Threat Defense デバイスの再起動の警告 （3 ページ）を参照してください。

注意 メンテナンス ウィンドウまたは中断の影響が最小限になる時間に展開することを強くお勧めします。

アプリケーション ディテクタの自動有効化

アプリケーション制御の実行時に必要なディテクタが無効になっている場合、システムは、ポリシーの展開時にシステムによって提供される適切なディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

ネットワーク検出ポリシーの変更によるアセットの再検出

ネットワーク検出ポリシーに変更を展開する場合、システムは、監視対象ネットワーク内のホストのネットワーク マップから MAC アドレス、TTL、およびホップ情報を削除してから、再検出を行います。また、影響を受ける管理対象デバイスは、まだ Firepower Management Center に送信されていない検出データを破棄します。

関連トピック

Snort® の再起動シナリオ （8 ページ）

Firepower Threat Defense デバイスの再起動の警告

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/Security Approver

展開時、展開ダイアログの [インスペクションの中断（Inspect Interruption）] 列に、設定を展開したときに Firepower Threat Defense デバイスで Snort プロセスが再起動するかどうかが示されます。Snort プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。トラフィックが中断されるか中断中にインスペクションなしで受け渡されるかどうかは、デバイスがトラフィックを処理する方法によって変わります。展開の続行、展開のキャンセル、および設定の変更を実行できます。または、展開によるネットワークへの影響が最小となる時間まで展開を遅らせることができます。

[インスペクションの中断（Inspect Interruption）] 列に [あり（Yes）] と表示されているときにデバイス設定リストを展開すると、Snort プロセスを再起動する特定の設定タイプは赤色と再起動アイコン（⛔）で強調表示されます。これらの設定にマウス ポインタを合わせると、設定を展開したときにトラフィックが中断される可能性があるというメッセージが表示されます。

次の表に、展開ダイアログでインスペクション中断の警告が表示される方法を示します。

表 *1:* 展開ダイアログにおけるインスペクション中断のインジケータ

タイプ（Type）	インスペクションの中断	説明
FTD	○	少なくとも1つの設定は、展開するとデバイスでインスペクションが中断します。また、デバイスがトラフィックを処理する方法によって、トラフィックが中断されることがあります。デバイス設定リストを展開して、詳細を確認できます。
	なし	展開されている設定は、デバイスのトラフィックを中断しません。
	不明	展開された設定によってデバイスのトラフィックが中断される可能性があるかどうかをシステムが判断できず、デバイスの横にデバイス警告アイコン（  ）が表示されます。 最初の展開の前の、ソフトウェア アップグレードの後に、または場合によってはサポート コール中に、不明ステータスが表示されます。
	 エラー	内部エラーにより、システムはステータスを特定できません。 操作をキャンセルして再度 [展開（Deploy）] をクリックすると、システムは [インスペクションの中断（Inspect Interruption）] ステータスを特定しなおすことができます。それでも問題が解決しない場合は、サポートにお問い合わせください。
センサー	--	センサーとして識別されるデバイスは Firepower Threat Defense デバイスではありません。設定を展開するとこのデバイスのトラフィックが中断されるかどうかの判断は行われません。

すべてのデバイス タイプの Snort プロセスを再起動する全設定の詳細については、展開またはアクティブ化された際に Snort プロセスを再起動する設定（12 ページ） を参照してください。

設定変更の展開

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/Security Approver

設定を変更したら、影響を受けるデバイスに展開します。メンテナンス ウィンドウで、またはトラフィック フローとインスペクションに対する中断の影響が最小限になる時間に、展開することを強くお勧めします。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。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。Snort® の再起動によるトラフィックの動作 （10 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（12 ページ）を参照してください。

始める前に

- 設定変更の展開に関する注意事項 （2 ページ）で説明されているガイドラインを確認してください。
- すべての管理対象デバイスが同じバージョンのセキュリティ ゾーン オブジェクトを使用していることを確認してください。セキュリティ ゾーン オブジェクトを編集している場合：Do not deploy configuration changes to any device until you edit the zone setting for interfaces on *all* devices you want to sync. すべての管理対象デバイスに同時に展開する必要があります。（セキュリティ ゾーン オブジェクトのリビジョンの同期を参照してください。）

手順

ステップ 1 Firepower Management Center メニュー バーで、[展開（Deploy）] をクリックします。

[ポリシーの展開（Deploy Policies）] ダイアログに、設定の期限が切れているデバイスがリストされます。ダイアログの上部の [バージョン（Version）] は、最後に設定変更を行った時期を示します。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [ソート（Sort）]：列ヘッダーをクリックすることで、デバイス リストをソートします。

Firepower Threat Defense デバイスへの展開時にトラフィック検査を中断させたりトラフィック自体を中断させる可能性のある設定を識別するために役立つ列については、Firepower Threat Defense デバイスの再起動の警告 （3 ページ）を参照してください。

すべてのデバイスへの展開時にトラフィック検査を中断させたりトラフィック自体を中断させる可能性のある設定については、展開またはアクティブ化された際に Snort プロセスを再起動する設定 （12 ページ）を参照してください。

- [展開（Expand）]：デバイス リストを展開して展開される設定変更を表示するには、プラス アイコン（⊞）をクリックします。システムは、期限切れのポリシーをインデックス（⏲）アイコンでマーキングします。

  [インスペクションの中断（Inspect Interruption）] 列のステータスに [あり（Yes）] と表示されている場合は、展開すると Firepower Threat Defense デバイスでインスペクション（および場合によってはトラフィック）が中断され、展開されたリストで中断の原因となった設定が赤色で強調表示されます。

- [フィルタ（Filter）]：デバイス リストをフィルタリングします。列ヘッダーの右隅にある矢印をクリックします。

  - [検査中断（Inspect Interruption）] 列：[フィルタ（Filters）] ドロップダウン メニューで、目的のフィルタ オプションを確認します。複数のオプションを選択できます。

    再起動に関する警告の詳細については、Firepower Threat Defense デバイスの再起動の警告 （3 ページ）を参照してください。

  - その他のすべての列：[フィルタ（Filters）] テキスト ボックスにテキストを入力し、Enter を押します。

  [フィルタ（Filters）] チェックボックスをオンまたはオフにして、フィルタをアクティブまたは非アクティブにします。

- 変更：右上の歯車アイコン（⚙）をクリックして、[列（Columns）] ドロップダウン リストから表示する列のチェックボックスをオンまたはオフにします。
- 調整：マウス カーソルを列ヘッダーの上に移動し、列をドラッグ アンド ドロップして希望の順序にします。

ステップ 3 [Deploy] をクリックします。

ステップ 4 展開する変更でエラーまたは警告がシステムによって識別された場合は、[選択した展開のエラーおよび警告（Errors and Warnings for the Selected Deployment）] ウィンドウに詳細が表示されます。

次の選択肢があります。

- [続行（Proceed）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [キャンセル（Cancel）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次のタスク

- （オプション）展開ステータスをモニタします。展開メッセージの表示を参照してください。
- 展開が失敗した場合は、設定変更の展開に関する注意事項 （2 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ （8 ページ）

デバイスへの既存の設定の再展開

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/Security Approver

既存（変更なし）の設定を単一の管理対象デバイスに強制展開できます。メンテナンス ウィンドウで、またはトラフィック フローとインスペクションに対する中断の影響が最小限になる時間に、展開することを強くお勧めします。

⚠

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。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。Snort® の再起動によるトラフィックの動作 （10 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（12 ページ）を参照してください。

始める前に

設定変更の展開に関する注意事項 （2 ページ）で説明されているガイドラインを確認してください。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 強制導入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。

ステップ 4 [全般（General）] セクション見出しの横にある編集アイコン（  ）をクリックします。

ステップ 5 [強制導入（Force Deploy）] 矢印（）をクリックします。

ステップ 6 [展開（Deploy）] をクリックします。

システムでは、展開中の設定で発生したエラーや警告が識別されます。[続行（Proceed）] をクリックすると、警告状態を解決せずに続行できます。ただし、システムがエラーを示している場合は、続行できません。

次のタスク

- （オプション）展開ステータスをモニタします。展開メッセージの表示を参照してください。
- 展開が失敗した場合は、設定変更の展開に関する注意事項 （2 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ （8 ページ）

Snort® の再起動シナリオ

管理対象デバイス上の *Snort* プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。 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。詳細はSnort® の再起動によるトラフィックの動作 （10 ページ）を参照してください。 また、Snort プロセスが再起動するかどうかに関係なく、展開時にリソース需要が高まった結果、いくつかのパケットがインスペクションを実行せずにドロップされることがあります。

次の表に示すいずれかのシナリオでは、Snort プロセスが再起動されます。

表 *2: Snort* 再起動のシナリオ

再起動のシナリオ	詳細情報
Snort プロセスの再起動が必要な特定の設定を展開した場合。	展開またはアクティブ化された際に Snort プロセスを再起動する設定 （12 ページ）
Snort プロセスを直ちに再起動するように設定を変更した場合。	変更により Snort プロセスがただちに再起動する場合 （14 ページ）
現在展開されている自動アプリケーション バイパス（AAB）設定のトラフィックをアクティブにした場合。	自動アプリケーション バイパスの設定

関連トピック

アクセス コントロール ポリシーの詳細設定
展開またはアクティブ化された際に Snort プロセスを再起動する設定 （12 ページ）

ポリシー適用中のトラフィックの検査

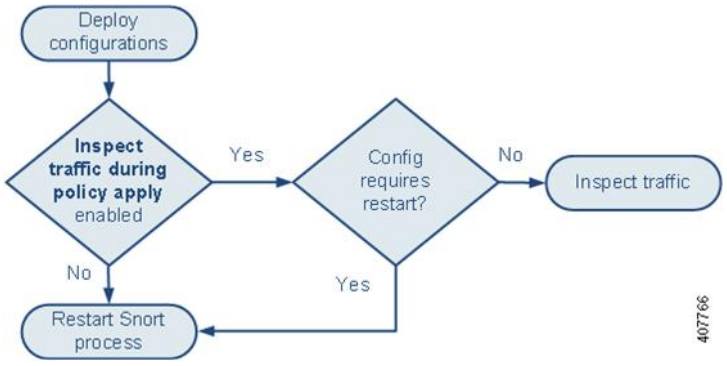
[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] は、管理対象デバイスが設定変更の展開時にトラフィックを検査できるようにするための詳細アクセス コントロール ポリシーの一般設定です。これは、展開する設定で Snort プロセスの再起動が不要な場合に限ります。このオプションは、次のように設定できます。

- [有効（Enabled）]：特定の設定で Snort 処理を再起動する必要な場合を除き、トラフィックは展開時に検査されます。

  展開する設定に Snort の再起動が必要でなければ、システムは現在展開されているアクセス コントロール ポリシーを使用してトラフィックを検査し、導入中に、展開しているアクセス コントロール ポリシーに切り替えます。

- [無効（Disabled）]：展開時にトラフィックは検査されません。Snort プロセスは展開時に必ず再起動されます。

次の図に、[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] を有効にした場合と無効にした場合の Snort の再起動の仕組みを示します。



注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。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。Snort® の再起動によるトラフィックの動作 （10 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定 （12 ページ）を参照してください。

Snort® の再起動によるトラフィックの動作

次の表に、Snort プロセスが再起動した場合のさまざまなデバイスのトラフィックの処理方法を示します。

表 *3: FTD* および *FTD* の仮想再起動トラフィックの影響

インターフェイスの設定	再起動によるトラフィックの動作
inline：**Snort Fail Open**：**Down**：disabled	dropped
inline：**Snort Fail Open**：**Down**：enabled	検査なしで受け渡される
preserve-connection が有効になっている場合（**configure snort preserve-connection enable**、デフォルト）はルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む） 6.3.x FMC で管理対象となる FTD はバージョン 6.3.x、6.2.3、6.2.0.2、または後続の 6.2.0.x パッチを実行している必要があります。 詳細については、Cisco Firepower Threat Defense コマンド リファレンスを参照してください。	既存の TCP/UDP フロー：インスペクションなしで受け渡される 新規 TCP/UDP フローとすべての非 TCP/UDP フロー：ドロップされる **preserve-connection** とハードウェア オフロード（**system support ssl-hw-offload**）の両方が有効になっている場合はすべての FTD 4100/9300 トラフィックがドロップされることに注意してください。 また、**preserve-connection** が有効になっている場合でも、次のトラフィックはドロップされることに注意してください。 • システムが **Do not decrypt** SSL ルールまたはデフォルト ポリシー アクションに一致するトラフィックにタグを付ける前に Snort がダウンした場合 （いくつかのハンドシェイク パケット交換の後にタグ付けが行われます） • プレーンテキスト、パススルー プレフィルタ トンネル トラフィック (**Analyze** ルール アクションまたは**Analyze all tunnel traffic** デフォルト ポリシー アクションと一致） • 復号化された TLS/SSL トラフィック • セーフ サーチ フロー • キャプティブ ポータル フロー

インターフェイスの設定	再起動によるトラフィックの動作
次のいずれかの状況の場合はルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む） • **preserve-connection** CLI コマンドが無効になっている（**configure snort preserve-connection disable**） • FTD バージョン（6.2.1、6.2.2、6.2.2.x、または 6.2.0.2 よりも前のバージョン）はこのコマンドをサポートしていません。	dropped
inline：tap mode	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし

表 *4 : 7000* および *8000* シリーズ、*NGIPSv* 再起動トラフィックの影響

インターフェイスの設定	再起動によるトラフィックの動作
inline：**Failsafe** enabled または disabled	インスペクションなしで受け渡される [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
inline：tap mode	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし
ルーテッド、スイッチド （7000 および 8000 シリーズのみ）	dropped

表 *5 : ASA FirePOWER Restart* トラフィックの影響

インターフェイスの設定	再起動によるトラフィックの動作
フェールオープンを伴うルーテッドまたはトランスペアレント	インスペクションなしで受け渡される
フェールクローズを伴うルーテッドまたはトランスペアレント	dropped

（注） 再起動中に Snort プロセスがダウンした場合のトラフィック処理に加え、フェールセーフ オプション（Firepower システムのインライン セット を参照）または Snort フェールオープンの [ビジー（Busy）] オプション（インラインセットを設定します。 を参照）の設定に応じて、トラフィックをインスペクションなしで通過させたり、または Snort プロセスがビジーのときにトラフィックをドロップしたりすることもできます。デバイスは、フェールセーフ オプションまたは Snort フェールオープン オプションの両方ではなくいずれかをサポートします。

（注） 設定の展開中に Snort プロセスがビジー状態になり、ダウンはしていない場合、総 CPU 負荷が 60 パーセントを超えると、ルーテッド、スイッチド、またはトランスペアレント インターフェイスでパケットがドロップすることがあります。

展開またはアクティブ化された際に Snort プロセスを再起動する設定

AAB 以外の構成を展開すると、Snort プロセスが再起動されます。AAB の展開自体には再起動が伴いませんが、パケットの遅延が大きすぎると、現在展開されている AAB 設定がアクティブになり、Snort プロセスが部分的に再起動されます。

アクセス コントロール ポリシーの詳細設定

- [ポリシー適用時にトラフィックのインスペクションを実行する（Inspect traffic during policy apply）] が無効な場合に展開します。
- SSL ポリシーを追加または削除します。

ファイル ポリシー（File Policy）

次のいずれかの構成の最初または最後を展開します。これらのファイル ポリシー構成を展開しても再起動は発生しませんが、非ファイル ポリシー構成を展開すると再起動が発生する可能性があることに注意してください。

- 次のいずれかの操作を行います。
  - 展開されたアクセス コントロール ポリシーに 1 つ以上のファイル ポリシーが含まれている場合は、[アーカイブを検査する（Inspect Archives）] を有効または無効にします。
  - [アーカイブを検査する（Inspect Archives）] が有効になっている場合は、最初のファイル ポリシー ルールを追加するか、または最後のファイル ポリシー ルールを削除します（[アーカイブを検査する（Inspect Archives）] が有意味であるためには 1 つ以上のルールが必要であることに注意してください）。
- [ファイルを検出（Detect Files）] または [ファイルをブロック（Block Files）] ルールで、[ストア ファイル（Store files）] を有効または無効にします。

- [マルウェア クラウドのルックアップ（Malware Cloud Lookup）] または [マルウェアをブロック（Block Malware）] ルール アクションと、分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[ダイナミック分析（Dynamic Analysis）] または [ローカル マルウェア分析（Local Malware Analysis）]）またはストア ファイル オプション（[マルウェア（Malware）]、[不明（Unknown）]、[クリーン（Clean）] または [カスタム（Custom）]）を組み合わせた最初のアクティブ ファイル ルールを追加するか、または最後のアクティブ ファイル ルールを削除します。

これらのファイル ポリシー構成をセキュリティ ゾーンまたはトンネル ゾーンに展開するアクセス コントロール ルールによって再起動が発生するのは、構成が次の条件を満たす場合だけであることに注意してください。

- アクセス コントロール ルールに含まれる送信元または宛先セキュリティ ゾーンは、ターゲット デバイス上のインターフェイスに関連付けられたセキュリティ ゾーンと一致する必要があります。
- アクセス コントロール ルールに含まれる宛先ゾーンが [任意（any）] でないかぎり、ルールに含まれる送信元トンネル ゾーンは、プレフィルタ ポリシーに含まれるトンネル ルールに割り当てられているトンネル ゾーンと一致する必要があります。

ID ポリシー

- SSL 復号化が無効になっている場合（つまり、アクセス コントロール ポリシーに SSL ポリシーが含まれていない場合）は、最初のアクティブ認証ルールを追加するか、または最後のルールを削除します。

  アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルール アクションが含まれるか、[パッシブ/VPN アイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれます。

ネットワーク ディスカバリ（Network Discovery）

- ネットワーク検出ポリシーを使用して、HTTP、FTP、または MDNS プロトコル経由で権限のないトラフィックベースのユーザ検出を有効または無効にします。

Device Management

- ルーティング：7000 または 8000 シリーズ デバイスにルーテッド インターフェイス ペアまたは仮想ルータを追加します。
- VPN：7000 または 8000 シリーズ デバイスで VPN を追加または削除します。

> ⚠ **注意** システムは、7000 または 8000 シリーズ デバイスの VPN を追加または削除したときに Snort プロセスが再起動することを警告しません。

- MTU：デバイス上のすべての非管理インターフェイスのうちの最大 MTU 値を変更します。
- 従来型デバイスの高可用性：高可用性状態共有オプションを変更します。 システムは、Snort プロセスがプライマリ デバイスとセカンダリ デバイスで再起動することを警告しません。
- 自動アプリケーション バイパス（AAB）：現在展開されている AAB 構成は、Snort プロセスの誤動作またはデバイスの誤設定により、単一のパケットが過度の処理時間を使用した場合にアクティブになります。その結果、Snort プロセスが部分的に再起動され、非常に大きい遅延が緩和されるか、または完全なトラフィックの停止が防止されます。この部分的な再起動により、デバイスがトラフィックをどのように処理するかに応じて、いくつかのパケットがインスペクションなしで通過するか、またはドロップされます。

変更点

- システム アップデート：新しいバージョンの Snort バイナリまたはデータ収集ライブラリ（DAQ）を含むソフトウェア アップデートの後に初めて構成を展開します。
- VDB：管理対象デバイスに適用可能な変更を含む、脆弱性データベース（VDB）更新のインストール後に初めて構成を展開します。そのため、インストールを開始するために Firepower Management Center を選択すると、警告メッセージが表示されます。展開ダイアログは、VDB 変更が保留中の場合、Firepower Threat Defense デバイスに関する付加的な警告を提供します。Firepower Management Center にのみ適用される VDB の更新では再起動が行われないため、更新を展開できません。

関連トピック

設定変更の展開 （5 ページ）
Snort® の再起動シナリオ （8 ページ）

変更により Snort プロセスがただちに再起動する場合

以下の変更を行うと、展開プロセスを経ることなく Snort プロセスが直ちに再起動されます。再起動がトラフィックにどのような影響を与えるかは、ターゲットデバイスがトラフィックを処理する方法によって異なります。詳細はSnort® の再起動によるトラフィックの動作（10 ページ）を参照してください。

- アプリケーションまたはアプリケーションディテクタに関する次の操作のいずれかを実行します。
  - システムまたはカスタム アプリケーション ディテクタを有効または無効にします。
  - アクティブ化されたカスタム ディテクタを削除します。
  - アクティブ化されたカスタム ディテクタを**保存して再アクティブ化**します。
  - ユーザ定義のアプリケーションを作成します。

この操作を続けると管理対象のすべてのデバイスで Snort プロセスが再起動するという警告メッセージが表示され、キャンセルが可能になります。再起動は、現在のドメインまたはその子ドメインのいずれかの管理対象デバイスで発生します。

- Firepower Threat Defense ハイ アベイラビリティ ペアの作成または解除：ハイ アベイラビリティ ペアの作成を続行すると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動するという警告メッセージが表示され、キャンセルが可能になります。
- 7000 または 8000 シリーズ ユーザ インターフェイスで Snort プロセスを再起動します（[システム（System）] > [設定（Configuration）] > [プロセス（Process）]）。確認メッセージが表示され、キャンセルすることができます。

ポリシーの比較

変更後のポリシーが組織の標準に準拠することを確かめたり、システム パフォーマンスを最適化したりする目的で、2 つのファイル ポリシーの間の違いや、保存済みポリシーと実行中のポリシーの間の違いを調べることができます。

比較できるポリシーのタイプは次のとおりです。

- DNS
- ファイル
- ヘルス
- アイデンティティ
- 侵入
- ネットワーク分析
- SSL

比較ビューには、両方のポリシーが並べて表示されます。2 つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

ポリシーの比較

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**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	機能に応じて異なる	機能に応じて異なる

手順

ステップ 1 比較するポリシーの管理ページにアクセスします。

- [DNS]：**[Policies]** > **[Access Control]** > **[DNS]**
- [ファイル（File）]：**[Policies]** > **[Access Control]** > **[Malware & File]**
- [状況（Health）]：**[System]** > **[Health]** > **[Policy]**
- [ID（Identity）]：**[Policies]** > **[Access Control]** > **[Identity]**
- [侵入（Intrusion）]：**[Policies]** > **[Access Control]** > **[Intrusion]**
- [ネットワーク分析（Network Analysis）]：**[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**

  （注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[Policies]** > **[Access Control]** > **[SSL]**

ステップ 2 [ポリシーの比較（Compare Policies）] をクリックします。

ステップ 3 [比較対象（Compare Against）] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[他のポリシー（Other Policy）] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。
- 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[実行中の設定（Running Configuration）] を選択します。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合、[ポリシー A（Policy A）] ドロップダウン リストと [ポリシー B（Policy B）] ドロップダウン リストから比較するポリシーを選択します。
- 実行中の設定を別のポリシーと比較する場合、[ポリシー B（Policy B）] ドロップダウン リストから 2 番目のポリシーを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 比較の結果を確認します。

- [比較ビューア（Comparison Viewer）]：比較ビューアを使用して、ポリシーの違いを個別に検索するには、タイトル バーの上にある [前へ（Previous）] または [次へ（Next）] をクリックします。
- [比較レポート（Comparison Report）]：2 つのポリシーの違いを示す PDF レポートを生成するには、[比較レポート（Comparison Report）] をクリックします。

ポリシー レポート

ほとんどのポリシーには、2 種類のレポートを生成することができます。単一のポリシーに関するレポートには、現在保存されているポリシー設定の詳細が記載されます。一方、比較レポートには、2つのポリシー間の違いだけがリストされます。単一ポリシー レポートは、ヘルス ポリシーを除くすべてのポリシー タイプについて生成できます。

（注） 侵入ポリシー レポートには基本ポリシーの設定とポリシー階層の設定が結合され、どちらが基本ポリシーまたはポリシー レイヤのどちらに基づく設定であるかは区別されません。

現在のポリシー レポートの生成

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）
機能に応じて異なる	機能に応じて異なる	任意（Any）	機能に応じて異なる	機能に応じて異なる

手順

ステップ 1 レポートを生成するポリシーの管理ページにアクセスします。

- アクセス制御—**[Policies]** > **[Access Control]**
- [DNS]：**[Policies]** > **[Access Control]** > **[DNS]**
- [ファイル（File）]：**[Policies]** > **[Access Control]** > **[Malware & File]**
- [状況（Health）]：**[System]** > **[Health]** > **[Policy]**
- [ID（Identity）]：**[Policies]** > **[Access Control]** > **[Identity]**
- [侵入（Intrusion）]：**[Policies]** > **[Access Control]** > **[Intrusion]**
- 7000 & 8000 シリーズ デバイスの NAT：**[Devices]** > **[NAT]**
- [ネットワーク分析（Network Analysis）]：**[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[Policies]** > **[Access Control]** > **[SSL]**

ステップ 2 レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。

失効ポリシー

Firepower システムは、失効したポリシーに赤色のステータス テキストでマークを付けます。このテキストには、ポリシーの更新を必要とするターゲットデバイスの数が示されます。失効ステータスをクリアするには、ポリシーをデバイスに再展開する必要があります。

ポリシーの再展開が必要な設定変更には次のものがあります。

- アクセス コントロール ポリシー自体の変更：アクセス コントロール ルール、デフォルト アクション、ポリシー ターゲット、セキュリティ インテリジェンス フィルタリング、前処理などの詳細オプションの変更。
- アクセス コントロール ポリシーが呼び出すポリシーの変更：SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、アイデンティティ ポリシー、または DNS ポリシー。
- 呼び出されるアクセス コントロール ポリシーで使用される再利用可能オブジェクトまたは設定の変更：
  - ネットワーク、ポート、VLAN タグ、URL、地理位置情報オブジェクト
  - セキュリティ インテリジェンス リストおよびフィード
  - アプリケーション フィルタまたはディテクタ
  - 侵入ポリシーの変数セット
  - ファイル リスト
  - 復号関連のオブジェクトとセキュリティ ゾーン
- システム ソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

Web インターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクト マネージャ（**[Objects]** > **[Object Management]**）を使用してセキュリティ ゾーンを変更できますが、デバイスの設定（**[Devices]** > **[Device Management]**）でインターフェイスのタイプを変更すると、ゾーンも変更され、ポリシーの再展開が必要になります。

次の更新では、ポリシーの再展開は**必要ありません**。

- セキュリティ インテリジェンス フィードへの自動更新およびコンテキスト メニューを使用したセキュリティ インテリジェンスのグローバル ブラックリストおよびホワイトリストへの追加
- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

限定的な導入のパフォーマンスに関する考慮事項

システムはホスト、アプリケーション、ユーザ検出データを使用することで、ネットワークの完全な最新プロファイルを作成できます。また、システムが侵入検知および防御システム（IPS）として機能して、ネットワーク トラフィックを分析して侵入およびエクスプロイトを検出し、オプションで問題のあるパケットをドロップすることもできます。

検出とIPSを組み合わせることで、ネットワーク アクティビティにコンテンツが提供され、次のような多くの機能を利用することができます。

- 侵害の影響フラグと表示。これによって、どのホストが特定のエクスプロイト、攻撃、またはマルウェアに対して脆弱であるかが示されます。
- アダプティブ プロファイルの更新と Firepower の推奨事項。これによって、宛先ホストに応じてトラフィックを個別に検査できます。
- 相関。これによって、影響を受けるホストに応じて別々に侵入（およびその他のイベント）に応答できます。

ただし、組織が IPS または検出のみを実行することを目的としている場合は、システムのパフォーマンスを最適化できる設定がいくつかあります。

侵入防御のない検出

検出機能では、ネットワーク トラフィックをモニタして、ネットワーク上のホストの数とタイプ（ネットワーク デバイスを含む）だけでなく、それらのホスト上のオペレーティング システム、アクティブなアプリケーション、およびオープン ポートを判断できます。管理対象デバイスをネットワークのユーザアクティビティをモニタするように設定することもできます。検出データを使用して、トラフィック プロファイリングを実行し、ネットワーク コンプライアンスを評価し、ポリシー違反に応答できます。

基本的な展開（検出と単純なネットワークベースのアクセス制御のみ）では、アクセス コントロール ポリシーの設定時にいくつかの重要なガイドラインに従うことで、デバイスのパフォーマンスを向上させることができます。

（注） それが単にすべてのトラフィックを許可する場合であっても、アクセスコントロールポリシーを使用する必要があります。ネットワーク検出ポリシーが実行できるのは、アクセス コントロール ポリシーが通過を許可したトラフィックを検査することのみです。

最初に、アクセスコントロールポリシーは複雑な処理を必要とせず、単純なネットワークベースの基準のみを使用してネットワーク トラフィックを処理することを確認します。次のすべてのガイドラインを実装する必要があります。これらのオプションのいずれかを誤って設定すると、パフォーマンス上の利点がなくなります。

- セキュリティ インテリジェンス機能を使用しないでください。入力されたグローバル ホワイトリストまたはブラックリストをポリシーのセキュリティインテリジェンスの設定から削除します。
- モニタ アクションまたはインタラクティブ ブロック アクションに、アクセス コントロール ルールを含めないでください。許可、信頼、およびブロック ルールのみを使用します。許可されたトラフィックは検出によって検査できますが、信頼されたトラフィックとブロックされたトラフィックは検査できないことに留意してください。
- アプリケーション、ユーザ、URL、ISE 属性、または位置情報ベースのネットワーク条件にアクセス コントロール ルールを含めないでください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。
- ファイル、マルウェア、または侵入インスペクションを実行するアクセス コントロール ルールを含めないでください。つまり、ファイルポリシーまたは侵入ポリシーをアクセス コントロール ルールに関連付けないでください。
- アクセスコントロールポリシーのデフォルトの侵入ポリシーが [アクティブなルールなし（No Rules Active）] に設定されていることを確認します。
- ポリシーのデフォルトアクションとして [ネットワーク検出のみ（Network Discovery Only）] を選択します。侵入インスペクションを実行するポリシーのデフォルトアクションを選択しないでください。

アクセス コントロール ポリシーと組み合わせて、ネットワーク検出ポリシーを設定して適用できます。このポリシーは、システムが検出データについて検査をするネットワーク セグメント、ポート、およびゾーンを指定し、ホスト、アプリケーション、およびユーザがセグメント、ポート、およびゾーンで検出されるかどうかを指定します。

関連トピック

デフォルトの侵入ポリシー

ディスカバリのない侵入防御

必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。検出を無効にするには、次のすべての変更を実装する必要があります。

- ネットワーク検出ポリシーからすべてのルールを削除します。
- 単純なネットワークベースの条件（ゾーン、IPアドレス、VLANタグ、およびポート）のみを使用してアクセス制御を実行します。

  どんな種類のセキュリティインテリジェンス、アプリケーション、ユーザ、URL、または地理位置情報の制御も行わないでください。検出データの保存を無効にできても、システムではそれらの機能を実装するためにデータを収集して検査する必要があります。
- デフォルトのグローバル リストなど、アクセス コントロール ポリシーのセキュリティ インテリジェンス設定からすべてのホワイトリストとブラックリストを削除することで、ネットワークと URL ベースのセキュリティ インテリジェンスを無効にします。
- DNSのデフォルトのグローバル ホワイトリストやDNSルールのグローバル ブラックリストなど、関連付けられている DNS ポリシー内のすべてのルールを削除または無効にすることで、DNS ベースのセキュリティ インテリジェンスを無効にします。

展開後、新たな検出はターゲットデバイス上で停止します。タイムアウトの設定に応じて、システムはネットワーク マップ内の情報を段階的に削除していきます。または、すべての検出データを即座に消去できます。