ユースケース - Cisco Secure Firewall Management Center で Snort 3 推奨事項を生成する

Snort 3 ルールの推奨事項

ルールの推奨事項は、ホスト環境に固有のルールを使用して侵入ポリシーを自動的に調整します。ネットワークに存在しない脆弱性のルールを無効にすることで、追加のルールを有効にしたり、現在のルールセットを調整できます。詳細については、Cisco Secure Firewall 推奨ルールの概要を参照してください。

動作の仕組み

Management Center は、パッシブ検出を通じて、IP アドレス、ホスト名、オペレーティングシステム、サービス、ユーザー、クライアントアプリケーションなどの詳細を含む、ネットワーク上のホストのデータベースを構築します。この情報に基づいて、システムは検出された各ホストに脆弱性をマッピングします。推奨機能は、このホストデータベースを使用して、環境に適用するルールを決定します。

Snort 3 には 4 つのセキュリティレベルがあり、それぞれが特定の Talos ポリシーに対応しています。その内容は次のとおりです。

- レベル 1：セキュリティよりも接続性を優先（Connectivity Over Security）
- レベル 2：セキュリティと接続性のバランスをとる（Balanced Security and Connectivity）
- レベル 3：接続性よりもセキュリティを優先（Security Over Connectivity）

- レベル 4：最大検出（Maximum Detection）

ネットワーク内のホストで検出されない脆弱性のルールを無効にするには、[ルールを無効にするための推奨事項を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオンにします。アラートの数が多いためにルールセットをトリミングする必要がある場合、またはインスペクションのパフォーマンスを向上させる必要がある場合にのみ、このオプションをオンにします。

メリット

- 推奨事項を設定することで、侵入ポリシーを調整して、ホスト環境に固有のルールを使用して特定のタイプの脅威をより効果的に検出できます。
- 推奨事項は、誤検出と検出漏れを減らすことで、より効率的で効果的なインシデント対応プロセスに役立ちます。

ビジネスシナリオの例

大規模な企業ネットワークで、主要な侵入検知および防御システムとして Snort 3 を使用しているとします。セキュリティへの脅威が急速に進化する状況では、堅牢なネットワークセキュリティ対策を採用する必要があります。セキュリティチームは、インシデント対応機能を強化したいと考えています。これを行う方法の 1 つは、ホストネットワークで検出された脆弱性に基づいて推奨事項またはルールセットを生成することです。これは、侵入ポリシーを最適化し、ネットワークをより効果的に保護するのに役立ちます。

ベストプラクティス

- 高品質で正確なホストデータが必要です。

  ネットワーク検出はパッシブな性質であるため、脅威防御デバイスは保護されたホストのできるだけ近くに配置する必要があります。これにより、脅威防御デバイスはこれらのホストで送受信されるネットワークトラフィックを監視し、ネットワークに存在するアプリケーション、サービス、および脆弱性に関する正確なデータを提供できます。
- デバイスは、正確なホストプロファイルを作成するために、水平方向（East-West）および垂直方向（North-South）のトラフィックフローを可視化する必要があります。
- スケジュールされたタスクを作成して、推奨事項を自動的に更新できます。

前提条件

- 推奨を生成するホストがシステムに存在することを確認します。

- 推奨事項に設定された保護されたネットワークは、システムに存在するホストにマッピングする必要があります。

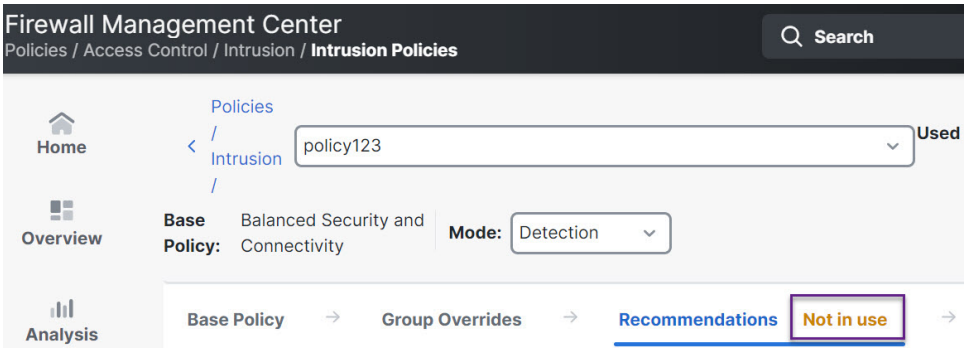
Snort 3 推奨事項の生成

手順

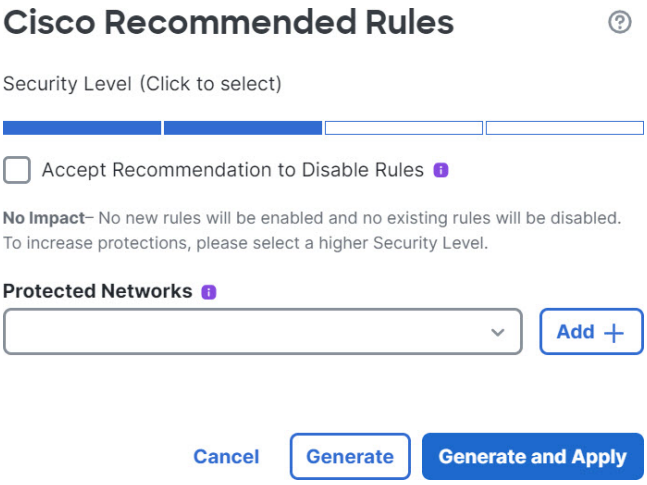
ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 対応する侵入ポリシーの [Snort 3バージョン（Snort 3 Version）] ボタンをクリックします。

ステップ 3 [推奨事項（未使用）（Recommendations (Not in Use)）] レイヤをクリックして、ルールの推奨事項を設定します。



[シスコ推奨ルール（Cisco Recommended Rules）] ウィンドウで、セキュリティレベルを設定できます。



ステップ 4 クリックして、セキュリティレベルを設定します。

ステップ 5 （オプション）ネットワーク内のホストで検出されない脆弱性用に記述されたルールを無効にするには、[ルールを無効にするための推奨事項を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオンにします。

アラートの数が多いためにルールセットをトリミングする必要がある場合、またはインスペクションのパフォーマンスを向上させる必要がある場合にのみ、このオプションを使用します。

ステップ 6 [保護されたネットワーク（Protected Networks）] ドロップダウンリストから、推奨事項によって調べる必要があるネットワークオブジェクトを選択します。デフォルトでは、選択されていない場合、IPv4 または IPv6 ネットワークが選択されます。

[追加+（Add+）] をクリックして、タイプが [ホスト（Host）] または [ネットワーク（Network）] の新しいネットワークオブジェクトを作成し、[保存（Save）] をクリックします。

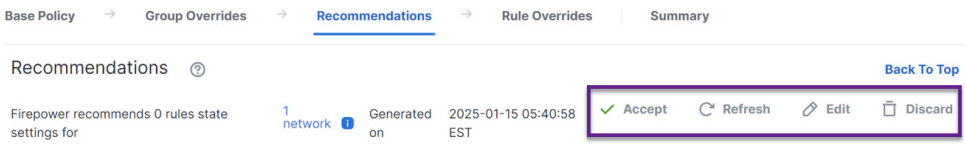
ステップ 7 推奨事項を生成および適用します。

- [生成（Generate）]：侵入ポリシーの推奨事項を生成します。このアクションは、[推奨ルール（未使用）（Recommended Rules (Not in use)）] の下にルールのリストを表示します。
- [生成して適用（Generate and Apply）]：侵入ポリシーの推奨事項を生成して適用します。このアクションは、[推奨ルール（未使用）（Recommended Rules (Not in use)）] の下にルールのリストを表示します。

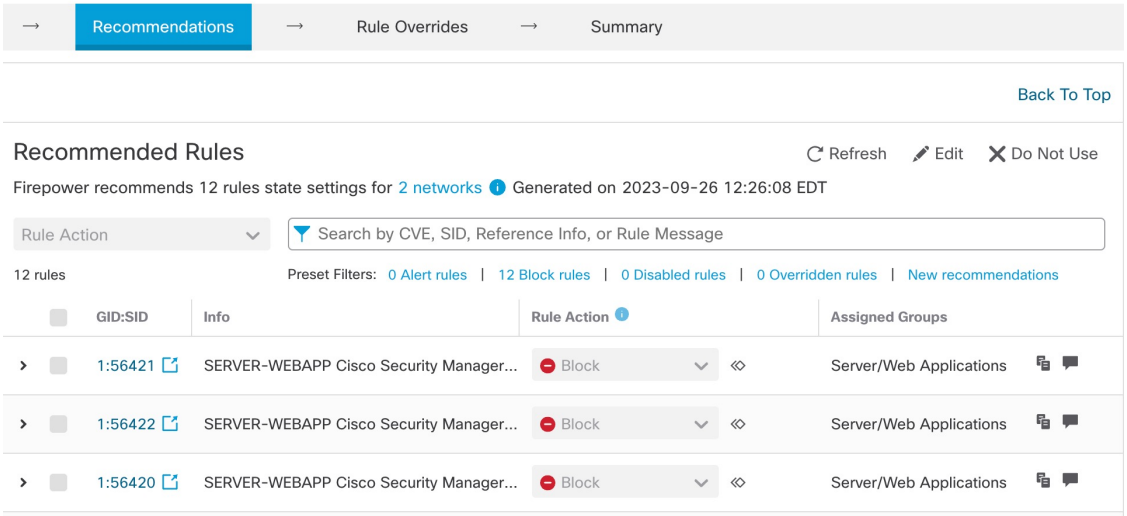
推奨事項が正常に生成されました。すべての推奨ルールと対応する推奨アクションが新しい推奨タブに表示されます。ルールアクションの事前設定フィルタは、新しい推奨事項に加えて、このタブでも使用できます。

ステップ 8 推奨事項を確認し、次のように適用します。

- [受け入れる（Accept）]：生成済みの侵入ポリシーの推奨事項を適用します。
- [更新（Refresh）]：侵入ポリシーのルール推奨事項を再生成および更新します。
- [編集（Edit）]：[推奨事項（Recommendations）] ダイアログボックスが開くので、推奨入力値を入力して推奨事項を生成します。
- [破棄（Discard）]：適用された推奨ルールを元に戻すか、ポリシーから削除し、[推奨事項（Recommendations）] タブも削除します。

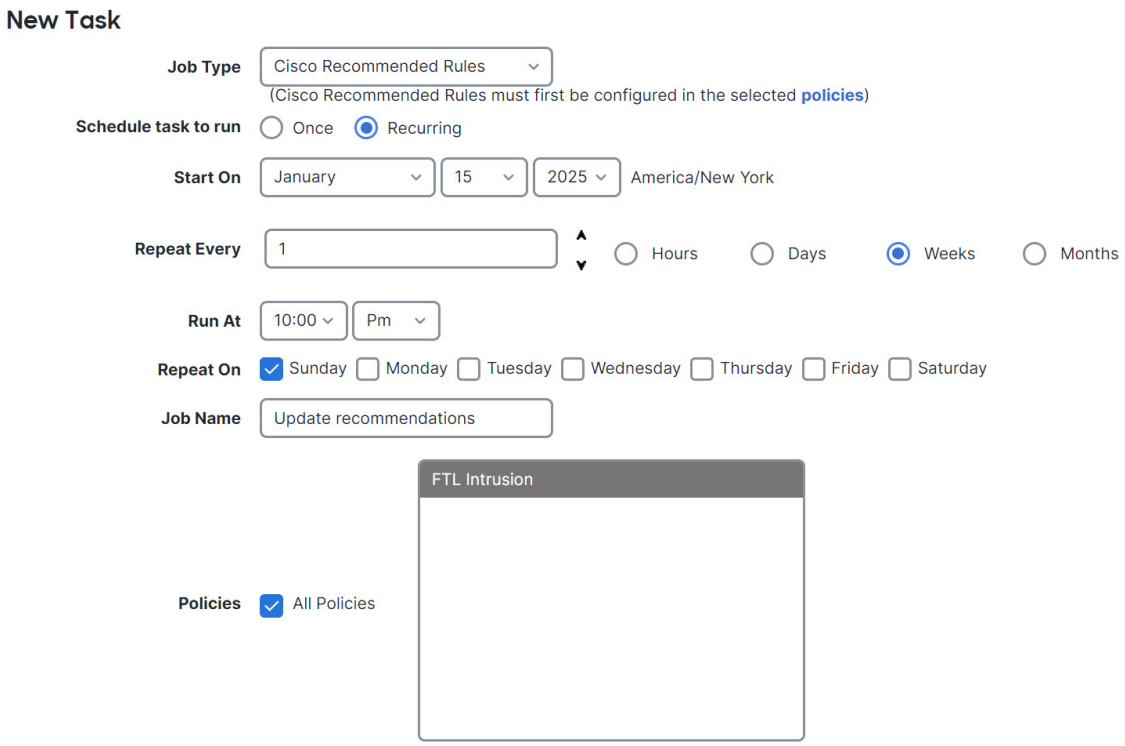


[すべてのルール（All Rules）] の [推奨ルール（Recommended Rules）] セクションに推奨ルールが表示されます。



ステップ 9 推奨事項を効果的に使用するには、定期的に更新する必要があります。次の手順に従ってください。

1. [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。
2. [タスクの追加（Add Task）] をクリックします。
3. [ジョブタイプ（Job Type）] ドロップダウンリストから [シスコ推奨ルール（Cisco Recommended Rules）] を選択します。
4. 必要に応じて、フィールドを更新してください。



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。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。

（注） このトピックでは、設定変更を展開する基本的な手順について説明します。手順を進める前に、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Deploy Configuration Changes*」トピックを参照し、変更を展開する上での前提条件と影響を理解しておくことを強く推奨します。

⚠

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。

手順

ステップ 1 Secure Firewall Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開（Deployment）] を選択します。

[GUI]ページには、期限切れの設定を持ち、ステータスが[保留中（Pending）]のデバイスのリストが表示されます。

- [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザーの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザーが表示されます。

  （注）
  削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断（Inspect Interruption）] 列には、展開時にデバイスでトラフィック インスペクションの中断が発生する可能性があるかどうかが示されます。

  デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィックインスペクションが中断されないことを示します。

- [最終変更時刻（Last Modified Time）] 列は、最後に設定変更を行った時刻を示します。
- [プレビュー（Preview）] 列では、次の展開の変更をプレビューできます。
- [ステータス（Status）] 列には、各展開のステータスが表示されます。

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。

- [検索（Search）] : [検索（Search）] ボックスのデバイス名、タイプ、ドメイン、グループ、またはステータスを検索します。
- [展開（Expand）] : 展開するデバイス固有の設定変更を表示するには、**Expand Arrow (›)** をクリックします。

  デバイスの横にあるチェックボックスをオンにすると、デバイスに加えられ、デバイスの下にリストされているすべての変更が展開のためにプッシュされます。ただし、**Policy selection** ( ) を使用して展開する個々のポリシーや特定の設定を選択し、残りの変更は展開せずに保持することができます。

  （注）

- [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、展開によって Firewall Threat Defense デバイスでインスペクションと、場合によってはトラフィックが中断されるときは、展開されたリストには中断の原因となった特定の設定が **Inspect Interruption** () で示されます。
- インターフェイスグループ、セキュリティゾーン、またはオブジェクトに変更がある場合、影響を受けるデバイスは、Firewall Management Center で失効として表示されます。これらの変更が有効になるようにするには、これらのインターフェイスグループ、セキュリティゾーン、またはオブジェクトを含むポリシーも、これらの変更とともに展開する必要があります。影響を受けるポリシーは、Firewall Management Center の [プレビュー（Preview）] ページに失効として表示されます。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ（Validation Messages）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

次の選択肢があります。

- [展開（Deploy）]：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。
- [閉じる（Close）]：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

展開中に展開が失敗した場合、その障害がトラフィックに影響を与える可能性があります。ただし、特定の条件によって異なります。展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。詳細については、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「Deploy Configuration Changes」のトピックを参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。