ネットワーク資産に応じた侵入防御の調整

この章では、Cisco Secure Firewall の推奨ルールと、Cisco Secure Firewall 推奨ルールの生成と適用について説明します。

LSP 更新での Snort 3 ルールの変更

通常の Snort 3 Lightweight Security Package（LSP）の更新中に、既存のシステム定義の侵入ルールが新しい侵入ルールに置き換えられることがあります。1 つのルールが複数のルールに置き換えられたり、または複数のルールが 1 つのルールに置き換えられたりする可能性があります。これは、結合または拡張されたルールに対してより適切な検出が可能な場合に発生します。管理を向上させるために、既存のシステム定義ルールの一部を LSP アップデートの一部として削除することもできます。

LSP 更新中にオーバーライドされたシステム定義ルールの変更に関する通知を受け取るには、[削除された Snort 3 ルールのユーザオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）] チェックボックスがオンになっていることを確認します。

[削除された Snort 3 ルールのユーザオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）] チェックボックスに移動するには、[**歯車**（Cog）]（⚙）をクリックして、**[設定（Configuration）] > [侵入ポリシー設定（Intrusion Policy Preferences）]** を選択します。

デフォルトでは、チェックボックスがオンになっています。このチェックボックスをオンにすると、LSP 更新の一部として追加される新しい置換ルールのルールオーバーライドが保持されます。通知は、[歯車（Cog）]（⚙）の横にある [通知（Notification）] アイコンの下にある [タスク（Task）] タブに表示されます。

Cisco Secure Firewall 推奨ルールの概要

侵入ルールの推奨事項を使用して、ネットワークで検出されたホストアセットに関連付けられている脆弱性を対象にすることができます。たとえば、オペレーティングシステム、サーバ、クライアント アプリケーション プロトコルなどです。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

システムは、侵入ポリシーごとに個別の推奨事項のセットを作成します。これにより、通常、標準テキストルールと共有オブジェクトルールのルール状態の変更が推奨されます。ただし、インスペクタやデコーダのルールの変更も推奨されています。

ルール状態の推奨事項を生成する場合は、デフォルト設定を使用するか、詳細設定を指定できます。詳細設定では次の操作が可能です。

- システムが脆弱性をモニタするネットワーク上のホストを再定義する。
- ルール オーバーヘッドに基づき、システムが推奨するルールに影響を与える。
- ルールを無効にする推奨事項を生成するかどうかを指定する。

推奨事項をすぐに使用するか、推奨事項（および影響を受けるルール）を確認してから受け入れることができます。

推奨ルール状態を使用することを選択すると、読み取り専用の Secure Firewall 推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されます。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。

システムは、次のような手動で設定されたルール状態を変更しません。

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる。
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる。

ヒント 侵入ポリシー レポートには、推奨状態と異なるルール状態を持つルールのリストを含めることができます。

推奨が絞り込まれた [ルール（Rules）] ページを表示している最中に、あるいは、ナビゲーション パネルまたは [ポリシー情報（Policy Information）] ページから [ルール（Rules）] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[ルール（Rules）] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。

（注） Cisco Talos Intelligence Group（Talos）は、システムによって提供されるポリシーでの各ルールの適切な状態を決定します。システムによって提供されるポリシーをベースポリシーとして使用し、システムがルールをCisco Secure Firewallの推奨ルール状態に設定できるようにすると、侵入ポリシーのルールは、ネットワークアセットに推奨された設定と一致します。

ネットワーク分析と侵入ポリシーの前提条件

Snort検査エンジンが侵入およびマルウェア分析のトラフィックを処理できるようにするには、Threat Defense デバイスに対して IPS ライセンスを有効にする必要があります。

ネットワーク分析、侵入ポリシーを管理し、移行タスクを実行するには、管理者ユーザーである必要があります。

Snort 3 での新しい Cisco Secure Firewall 推奨事項の生成

侵入ポリシーのCisco Secure Firewall推奨事項を生成し、ここに記載されている手順に従って、推奨された新しいルール設定を Snort 3 に作成します。ルールのオーバーヘッドは、Snort 3 で選択したしきい値ポリシーに基づいて**セキュリティレベル**として解釈されます。推奨されるアクションが、選択したセキュリティレベルに基づいていて、それがベースポリシーよりも高い場合、推奨されるのはイベントの生成だけではありません。

Secure Firewall 推奨事項を設定する前に、以下にリストされている 3 つのポイントのうちどれが目標に最も近いかを尋ねる必要があります。

- 保護の強化：ホストデータベースで見つかった脆弱性に基づいて追加のルールを有効にし、ルールを自動的に無効にしません。これにより、ルールセットが大きくなる可能性があります。
- 保護の集中：ホストデータベースで見つかった脆弱性に基づいて追加のルールを有効にし、既存のルールを無効にします。これにより、検出された脆弱性に応じてルールの数を増減できます。
- より高い効率：現在有効になっているルールセットを使用し、ホストデータベースで見つからない脆弱性のルールを無効にします。これにより、有効なルールセットが小さくなる可能性があります。

応答に基づく、推奨アクションは次のとおりです。

- 推奨事項を次に高いセキュリティレベルに設定し、無効化ルールのチェックを外します。
- 推奨事項を次に高いセキュリティレベルに設定し、無効化ルールを確認します。
- 推奨事項を現在のセキュリティレベルに設定し、無効化ルールを確認します。

始める前に

Secure Firewall 推奨事項には、次の要件があります。

- 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。

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

ステップ 2 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。[開始（Start）] をクリックします。

[Secure Firewallルールの推奨事項（Firepower Rule Recommendations）] ウィンドウでは、次の項目を設定できます。

- [セキュリティレベル（Security Level）]：クリックして、セキュリティレベルを選択します。必要に応じて、[ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオンにして、入力セキュリティレベルおよび保護されたネットワークで有効になっていないルールを無効にできます。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、このオプションを有効にします。セキュリティレベルは次のとおりです。
  - セキュリティレベル 1：セキュリティよりも接続性を優先（Connectivity Over Security）

    [影響なし（No Impact）]：新しいルールは有効にならず、既存のルールも無効になりません。保護を強化するには、より高いセキュリティレベルを選択してください。

    [セキュリティの低減（Lower Security）]（チェックボックスがオン）：検出されたホストの潜在的な脆弱性に一致する Connectivity Over Security ルールセットのルールを除き、すべてのルールが無効になります。代わりにベースポリシーを調整することを推奨します。

  - セキュリティレベル 2：バランスのとれた接続性よりもセキュリティを優先（Balanced Security Over Connectivity）

    [影響なし（No Impact）]：新しいルールは有効にならず、既存のルールも無効になりません。保護を強化するには、より高いセキュリティレベルを選択してください。

    [より高い効率（Higher Efficiency）]（チェックボックスがオン）：検出されたホストの潜在的な脆弱性に一致する既存のルールを保持し、ネットワークで検出されなかった脆弱性に関するルールを無効にします。

  - セキュリティレベル 3：接続性よりもセキュリティを優先（Security Over Connectivity）

    [セキュリティの向上（Increased Security）]：Maximum Detection ルールセットに基づいて、検出されたホストの潜在的な脆弱性に一致する追加のルールを有効にします。

    [集中型セキュリティ（Focused Security）]（チェックボックスがオン）：Security Over Connectivity ルールセットに基づいて、検出されたホストの脆弱性に一致する追加のルールを有効にし、検出されたホストの潜在的な脆弱性に一致しない既存のルールを無効にします。

- セキュリティレベル 4：最大検出（Maximum Detection）

  [セキュリティの向上（Increased Security）]：Security Over Connectivity ルールセットに基づいて、検出されたホストの潜在的な脆弱性に一致する追加のルールを有効にします。

  [集中型セキュリティ（Focused Security）]（チェックボックスがオン）：Maximum Detection ルールセットに基づいて、検出されたホストの脆弱性に一致する追加のルールを有効にし、検出されたホストの潜在的な脆弱性に一致しない既存のルールを無効にします。

  （注） Maximum Detection ルールは非常に多くのルールを有効にするため、パフォーマンスに影響する可能性があります。実稼働環境に導入する前に、この設定を確認してテストすることをお勧めします。

- [保護されたネットワーク（Protected Networks）]：モニタ対象のネットワークまたは個々のホストを指定して、推奨事項を調べます。ドロップダウンリストから、1 つ以上のシステムまたはカスタム定義のネットワークオブジェクトを選択できます。デフォルトでは、IPv4 ネットワークまたは IPv6 ネットワークが選択されます（選択されていない場合）。

  重要 Secure Firewall ルールの推奨事項は、ネットワーク検出に依存します。保護されたネットワークは、ネットワーク検出ポリシーで構成された範囲内で検出されたすべてのホストに適用されます。詳細については、『*Cisco Secure Firewall Management Center Device Configuration guide*』の「Network Discovery Policies」の章を参照してください。

  [追加+（Add+）]ボタンをクリックして、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 4 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（使用中）（Recommended Rules (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 5 推奨事項を確認し、それに応じて適用することを選択できます。

- [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。
- [すべて削除（Remove All）]：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、推奨タブも削除します。

[すべてのルール（All Rules）] の下に、推奨ルールを表示する [推奨ルールRecommended Rules] セクションがあります。

（注） 侵入ルールの最終アクションは、ルールアクションの優先順位に基づいて適用されます。次に、ルールアクションの優先順位を示します。

[ルールのオーバーライド（Rule Override）] > [生成された推奨事項（Generated Recommendations）] > [グループのオーバーライド（Group Override）] > [ベースポリシーのデフォルトアクション（Base Policy Default Action）]

推奨事項が有効になっている場合、Management Center では現在の状態（グループのオーバーライド、ベースポリシー、および推奨の設定）が考慮されます。アクションの優先順位は次のとおりです。

[パス（Pass）] > [ブロック（Block）] > [拒否（Reject）] > [ドロップ（Drop）] > [書き換え（Rewrite）] > [アラート（Alert）]

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。

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。