ポリシーアナライザとオプティマイザを使用したポリシー異常の分析、検出、および修復

ポリシーアナライザおよびオプティマイザ について

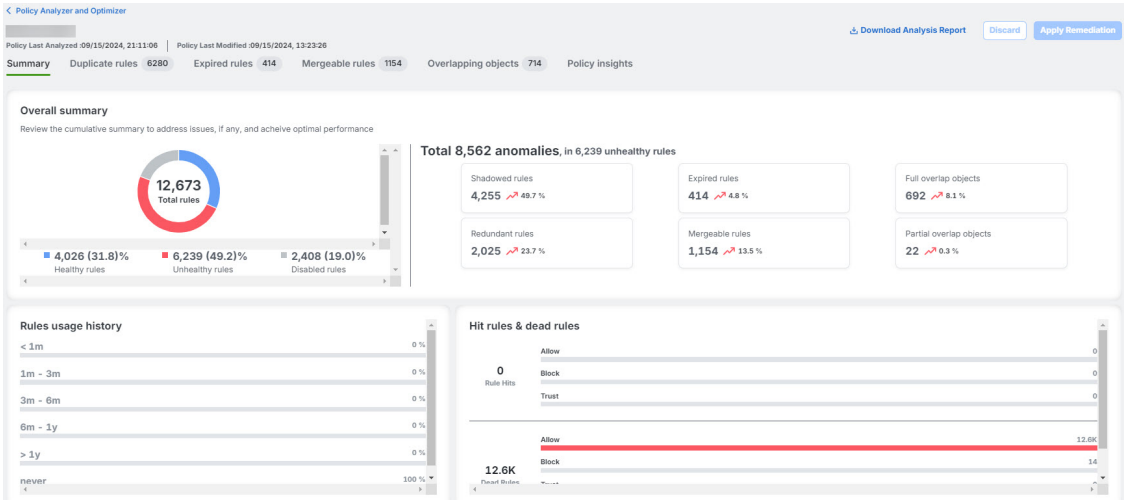
広範なアクセス コントロール ポリシーがある Cisco Secure Firewall Threat Defense デバイス、特にファイアウォールの移行プロセスで生成されたポリシーには、多数の重複ルールまたはシャドウルールが存在する可能性があります。最適化されていないルールセットを含むこのように拡張されたポリシーは、デバイスメモリの過剰な消費、ルールのロードの遅延、検索時間の延長につながり、セキュリティポリシーの適用が非効率になり、ネットワーク速度が低下し、展開期間が長くなる可能性があります。

このような状況に対処するために、Security Cloud Control には ポリシーアナライザおよびオプティマイザ が用意されています。これは、セキュリティポリシーを分析し、異常を検出し、ポリシーを最適化するために実行できる修復に関する推奨事項を提供できる、インテリジェントなクラウドサービスであり、結果としてファイアウォールのパフォーマンスが向上します。ポリシーアナライザおよびオプティマイザ は、Security Cloud Control にオンボードされている ク

ラウド提供型 Firewall Management Center と オンプレミス Firewall Management Center の両方のポリシーを分析できます。さらに、次のことを実行できます。

- 分析の概要や集約ヒットカウントに基づくポリシーのインサイトなど、ポリシーの正常性情報を包括的に可視化します。
- スケジュールされた間隔で、または必要に応じてポリシーを定期的に分析します。
- ルールの異常（ルールの重複、ルール内のオブジェクトの重複、期限切れのルールなど）を検出します。

図 *1*: 分析の概要



管理者の便宜のために、Security Cloud Control の [サービス（Services）] ページ、左側のペインの **[インサイト（Insights）]** > **[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）]**、および クラウド提供型 Firewall Management Center と オンプレミス Management Center の [アクセス制御（Access Control）] ポリシーページから ポリシーアナライザおよびオプティマイザ を起動できます。

分析、修復、およびレポート

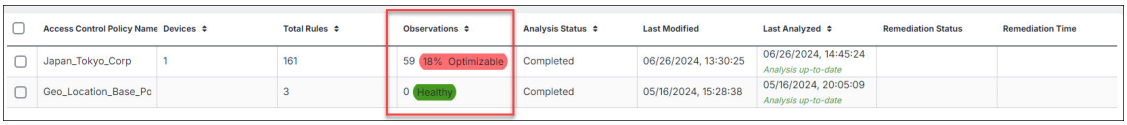
ポリシーアナライザおよびオプティマイザは、分析、修復、およびレポートのサービスを実行します。

分析

ポリシーアナライザおよびオプティマイザ は、ポリシーに対して クラウド提供型 Firewall Management Center および オンプレミス Management Center をポーリングし、ポリシーアナライザおよびオプティマイザ ページに表示します。[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] ページを開くには、左側のペインで **[管理（Administration）]** > **[Firewall Management Center]** をクリックし、[クラウド提供型FMC（Cloud-Delivered FMC）] または任意の オンプレミス Management Center を選択し、右側のペインで [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] を選択します。または、Security Cloud Control の

左側のペインで、**[インサイトとレポート（Insights & Reports）]**>**[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）]** を選択します。左上隅の [データソース（Data Source）] タブから、[クラウド提供型FMC（Cloud-Delivered FMC）] または任意の オンプレミス Management Center を選択します。

新しいアクセス コントロール ポリシーを作成した場合、またはポリシーをインポートした場合、ポリシーアナライザおよびオプティマイザによってポリシーが識別されるまでに時間がかかります。識別されると、ポリシー分析を手動でトリガーできます。24時間ごとに実行される自動分析を待つこともできます。分析が完了すると、ポリシーアナライザおよびオプティマイザ は、ポリシー内のルールの数、最適化できるポリシーの割合、および [ルールの正常性の概要（Rule Health Summary）]、[ルールの最新使用状況（Rule Last Usage）]、[ルールヒットとデッドルール（Rule Hits and Dead Rules）] などの情報を含む詳細な概要に関するインサイトを提供します。



（注） [観測内容（Observations）] 列の [最適化可能（Optimizable）] の割合は、推奨される修復が適用された場合に最適化できるポリシー内のルール数の概算値です。

修復

ポリシー分析の概要には、セキュリティポリシーの正常性が示されており、ポリシーに適用する ポリシーアナライザおよびオプティマイザ によって提案された修復を選択できます。推奨される修復を使用して、重複ルール、重複するオブジェクト、期限切れのルール、および同様の許可およびブロック設定があるマージルールを無効化または削除できます。それらのルールは 1 つのルールにマージできます。ヒットカウントデータは、[ポリシーインサイト（Policy Insights）] タブに表示されます。[修復の適用（Apply Remediation）] を選択すると、選択した修復がポリシーに適用されます。

レポート

分析されたポリシーの詳細レポートを使用できます。ポリシーに修復が適用されると、修復レポートが利用可能になります。修復レポートには、存在していたポリシーの異常と適用された修復の統合リストが含まれており、PDF としてダウンロードできます。

ポリシーアナライザおよびオプティマイザを使用するための前提条件

- オンプレミス Firewall Management Center はバージョン 7.2 以降であり、Security Cloud Control にオンボードされている必要があります。分析するポリシーが少なくとも 1 つのデバイスに関連付けられていることを確認します。
- オンプレミス Firewall Management Center バージョン 7.6 以降は、Cisco Security Cloud と統合する必要があります。オンプレミス Firewall Management Center は、Cisco Security Cloud 統合の一環として選択した Security Cloud Control テナントにオンボードされます。

ポリシーアナライザおよびオプティマイザライセンスの要件

ポリシーアナライザおよびオプティマイザには、追加のライセンスは不要です。Security Cloud Control 基本サブスクリプションの一部として提供されます。

クラウド提供型 Firewall Management Center 用のポリシーアナライザおよびオプティマイザ の有効化

ポリシーアナライザおよびオプティマイザはデフォルトでクラウド提供型 Firewall Management Center に対して有効になっています。これを使用して クラウド提供型 Firewall Management Center のアクセスポリシーを分析するには、次の手順を実行します。

手順

ステップ 1 左側のペインで、**[管理（Administration）]** > **[Firewall Management Center]** をクリックします。

ステップ 2 クラウド提供型 Firewall Management Center がデフォルトで選択された状態で [サービス（Services）] ページが開きます。

ステップ 3 右側のペインの [システム（System）] の下にある [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] をクリックします。

クラウド提供型 Firewall Management Center にアクセス コントロール ポリシーが表示されます。分析対象のポリシーを選択したり、分析済みのポリシーの詳細を表示したりできます。

Security Cloud Control 管理対象 オンプレミス Firewall Management Center 用の ポリシーアナライザおよびオプティマイザ の有効化

オンプレミス Firewall Management Center バージョン 7.2 以降を使用している場合は、SecureX と統合し、オンプレミス Management Center を Security Cloud Control にオンボードし、**[管理（Administration）] > [Firewall Management Center]**に移動し、オンプレミス Management Center を選択し、右側のペインの [システム（System）] で [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] を選択します。詳細については、「オンプレミス Firewall Management Centerのオンボード」を参照してください。

オンプレミス Management Center バージョン 7.6 で ポリシーアナライザおよびオプティマイザを使用する場合は、次の手順を実行します。

手順

ステップ 1 オンプレミス Management Center で、**[統合（Integration）] > [Cisco Security Cloud]** に移動します。

ステップ 2 オンプレミス Management Center を Cisco Security Cloud と統合していない場合は、[Cisco Security Cloudの有効化（Enable Cisco Security Cloud）] をクリックし、手順に従います。クラウド統合を承認するには、既存の Security Cloud Control テナントを選択するか、新しいテナントをプロビジョニングすると、クラウド統合が成功した後に オンプレミス Management Center がオンボードされます。

ステップ 3 オンプレミス Management Center を Cisco Security Cloud と統合したら、[ポリシーアナライザとオプティマイザの有効化（Enable Policy Analyzer and Optimizer）] チェックボックスをオンにして、[保存（Save）] をクリックします。

ステップ 4 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** に移動します。

ステップ 5 ポリシーを選択し、[ポリシーの分析（Analyze Policy）] をクリックします。[異常（Anomaly）] 列に [進行中（In Progress）] と表示され、分析が完了すると、異常の数と最適化可能なポリシーの割合が表示されます。

ステップ 6 割合をクリックすると、オンプレミス Management Center が登録されている Security Cloud Control テナントの [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] ページが相互起動されます。

ポリシー分析

クラウド提供型 Firewall Management Center をプロビジョニングするか、オンプレミス Firewall Management Center を Security Cloud Control テナントにオンボードし、ポリシーを作成したら、ポリシーアナライザおよびオプティマイザを使用してポリシーの分析を開始できます。詳細に

ついては、「Onboard an オンプレミス Firewall Management Center」および「Enable クラウド提供型 Firewall Management Center on Your Security Cloud Control tenant」を参照してください。

ここでは、ポリシーのさまざまな分析方法について説明します。

クラウド提供型 Firewall Management Center ポリシーの分析

Security Cloud Control テナントで クラウド提供型 Firewall Management Center がすでにプロビジョニングされている場合は、すぐにポリシーの分析を開始できます。Security Cloud Control で クラウド提供型 Firewall Management Center をプロビジョニングするには、「Enable クラウド提供型 Firewall Management Center on Your Security Cloud Control」を参照してください。

（注） 新しいポリシーを作成すると、ポリシーアナライザおよびオプティマイザがポリシーの詳細を取得し、[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] に表示されるまでに時間がかかる場合があります。右上隅にある更新（ ）ボタンをクリックして、ページを手動で更新して新しいポリシーを表示します。

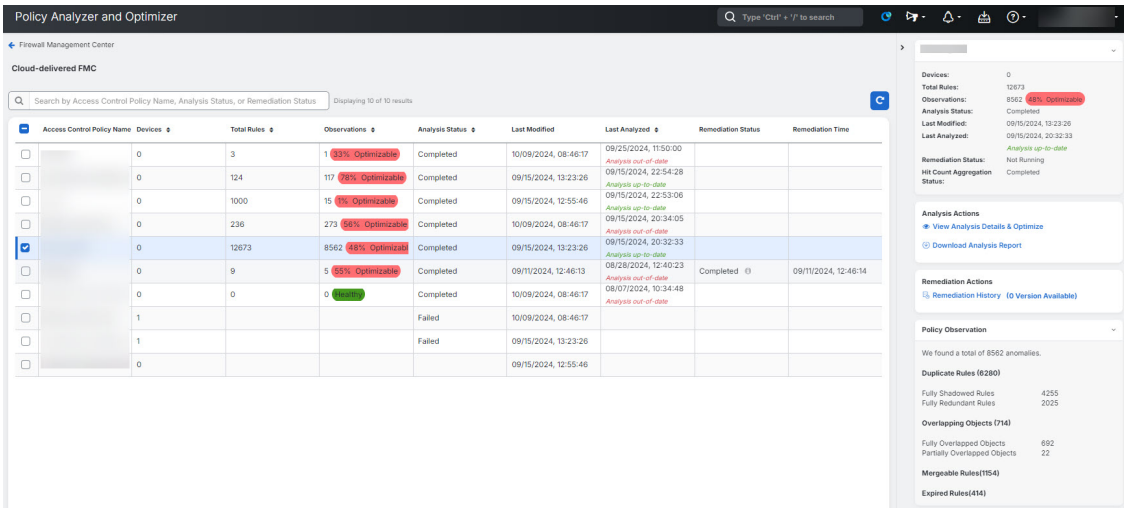
手順

ステップ 1 Security Cloud Control の左側のナビゲーションウィンドウから、**[管理（Administration）] > [Firewall Management Center]**に移動します。[クラウド提供型FMC（Cloud-Delivered FMC）] がデフォルトで選択されている [サービス（Services）] ページが表示されます。

ステップ 2 右側のペインの [システム（System）] の下にある [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] をクリックします。

または、左側のペインで、**[インサイトとレポート（Insights & Reports）] > [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）]** を選択します。左上隅の [ポリシーを表示（Showing policy for）] オプションに、表示されているデバイスのポリシーが表示されます。クリックして、クラウド提供型 Firewall Management Center と他の オンプレミス Firewall Management Center を切り替えます。

ステップ 3 分析済みポリシーの場合、ポリシーアナライザおよびオプティマイザには、[ルールの総数（Total Rules）]、[観測内容（Observations）]、[分析ステータス（Anaysis Status）]、および [最終変更日時（Last Modified）] と [最終分析日時（Last Analyzed）] のタイムスタンプを含む分析の概要が表示されます。ポリシーを選択すると、右側のペインにも詳細が表示されます。



ステップ 4 分析の詳細を表示するか、または再分析するポリシーを選択します。

ポリシーアナライザおよびオプティマイザ では 24 時間ごとにすべてのポリシーが自動的に分析されるため、すべてのポリシーがすでに分析されていて、詳細を確認できる可能性は高いです。

ステップ 5 別の分析を手動でトリガーするには、[ポリシーの再分析（Re-analyze Policy）] をクリックします。

オンプレミス Firewall Management Center ポリシーの分析

ポリシーアナライザおよびオプティマイザ を使用してオンプレミス Firewall Management Center バージョン 7.2 以降のポリシーを分析するには、オンボード方法として [Cisco Security Cloudからの自動検出（Auto discover from Cisco Security Cloud）] または [ログイン情報の使用（Use Credentials）] を使用して、Security Cloud Control にポリシーをオンボードする必要があります。オンプレミス Firewall Management Center バージョン 7.6 の場合は、Cisco Security Cloud に統合する必要があります。統合することで、オンプレミス Firewall Management Center が Security Cloud Control テナントにオンボードされます。開始する前に、次のことを確認してください。

- オンプレミス Firewall Management Center をオンボード後、**[管理（Administration）]** > **[Firewall Management Center]**でステータスが [アクティブ（Active）] であることを確認します。
- **[統合（Integration）]** > **[Cisco Security Cloud]** に移動して、Cisco Security Cloud と統合した後で [ポリシー分析と最適化を有効にする（Enable Policy Analysis & Optimization）] をオンにします。
- オンプレミス Firewall Management Center をオンボードしたばかりの場合、またはすでにオンボードされている オンプレミス Firewall Management Center で新しいポリシーを作成またはインポートした場合は、ポリシーアナライザおよびオプティマイザ がポリシーを取得するまで待ちます。
- ポリシーの分析は手動でトリガーできます。また、スケジュールされた自動分析の一部として自動的に分析できます。

手順

ステップ 1 Security Cloud Control の左側のナビゲーションウィンドウから、**[管理（Administration）]** > **[Firewall Management Center]**に移動します。[クラウド提供型FMC（Cloud-Delivered FMC）] がデフォルトで選択されている [サービス（Services）] ページが表示されます。

ステップ 2 ポリシーを分析する オンプレミス Firewall Management Center を選択します。

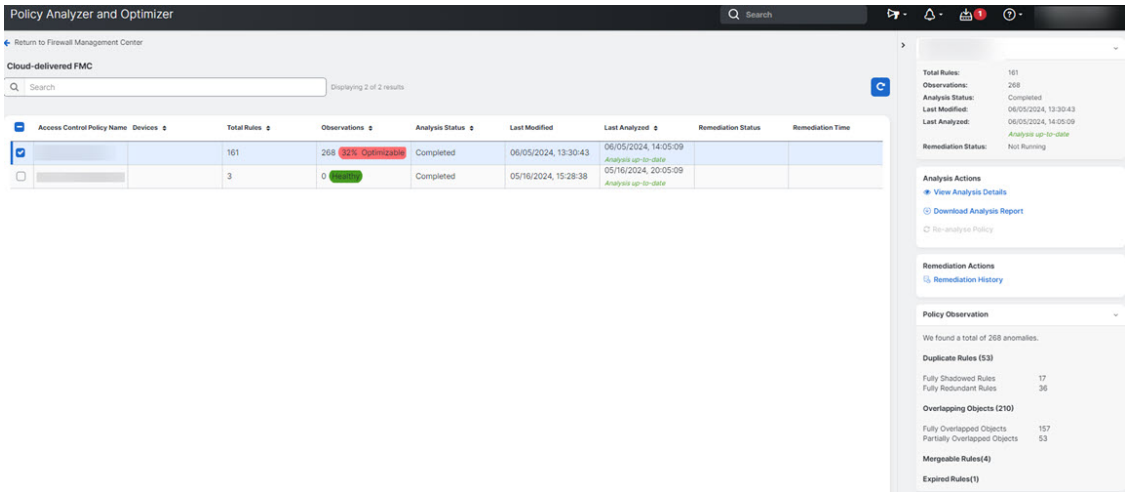
ステップ 3 右側のペインの [システム（System）] の下にある [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] をクリックします。

または、左側のペインで、**[インサイトとレポート（Insights & Reports）]** > **[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）]** を選択します。左上隅の [ポリシーを表示（Showing policy for）] オプションに、表示されているデバイスのポリシーが表示されます。クリックして、クラウド提供型 Firewall Management Center と他の オンプレミス Firewall Management Center を切り替えます。

ステップ 4 分析済みポリシーの場合、ポリシーアナライザおよびオプティマイザには、[ルールの総数（Total Rules）]、[観測内容（Observations）]、[分析ステータス（Anaysis Status）]、および [最終変更日時（Last Modified）] と [最終分析日時（Last Analyzed）] のタイムスタンプを含む分析の概要が表示されます。ポリシーを選択すると、右側のペインにも詳細が表示されます。

ポリシーレポート

ポリシーが分析され、準備ができると、[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] ページの [分析ステータス（Analysis Status）] が [完了（Completed）] になり、[観測内容（Observations）] 列に、ポリシーが正常であるか、最適化可能であるかが表示されます。

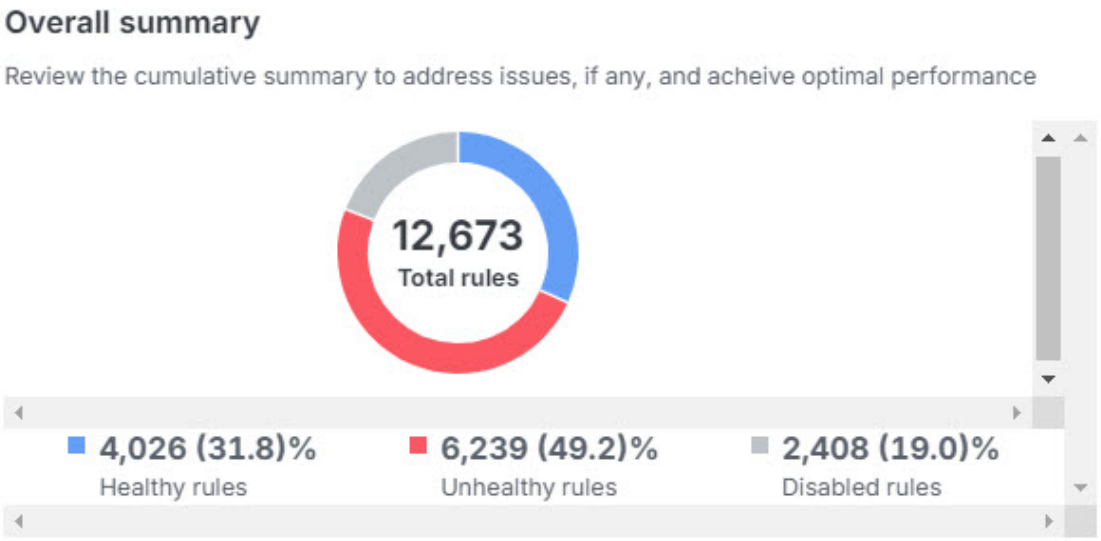


ポリシーを選択して、分析に関する詳細を右側のペインに表示します。[分析の詳細の表示（View Analysis Details）]、[分析レポートのダウンロード（Download Analysis Report）]、および [修復履歴（Remediation History）] を表示できます。

ポリシー分析の概要

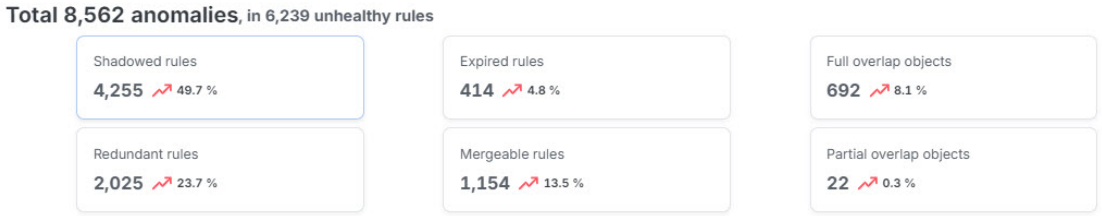
[概要（Summary）] タブには、次のルール情報が円グラフと棒グラフで表示されます。

[ルールの正常性の概要（Rule Health Summary）]：円グラフを使用して、正常、無効、期限切れ、および異常を含むルールの数に関するインサイトが表示されます。円グラフの一部にカーソルを合わせると、ルールの割合も表示できます。

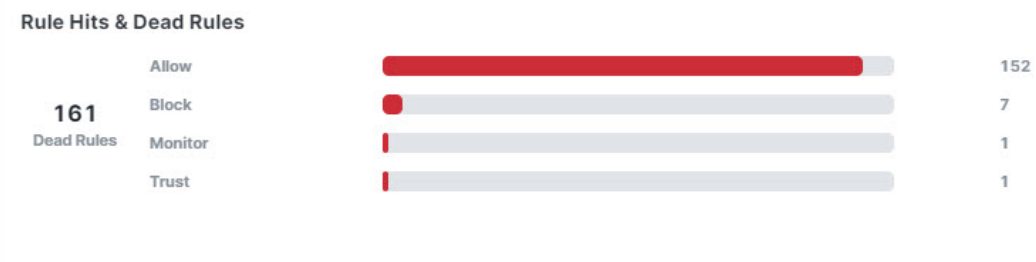


[ルールの最新使用状況（Rule Last Usage）]：最新のルールの使用状況に関するインサイトが期間とともに表示されます。

[異常があるルール（Rules with Anomalies）]：棒グラフを使用して、異常があるルールの数に関するインサイトが表示されます。バーにカーソルを合わせると、異常があるルールの数が表示されます。



[ルールヒットとデッドルール（Rule Hits and Dead Rules）]：許可、ブロック、監視、信頼などのルールタイプについて、期限切れのルールのヒットカウントに関するインサイトが表示されます。



重複ルール

[重複ルール（Duplicate Rules）] タブには、異常のあるシャドウルールと冗長ルールが一覧表示されます。

- [完全シャドウルール（Fully Shadowed Rule）] は先行する別のルールによってシャドウされるために、ネットワークトラフィックを評価しないルールです。
- [完全冗長ルール（Fully Redundant Rule）] は、別のより大きなルールの一部であり、このルールで実行する必要があるトラフィック評価はすでに別のルールによって実行されているため、この冗長ルールを削除してもネットワークトラフィックには影響しません。

すべての完全シャドウルールや完全冗長ルールを無効化または削除することを選択できます。

（注） 各観測値を展開して、ルールが大きいために冗長になっているルールのリストを確認します。リスト内の各ルールは、一連の属性とともに表示されます。右上の [設定（Settings）] ボタンをクリックして、ルールとともに表示するルール属性を選択します。

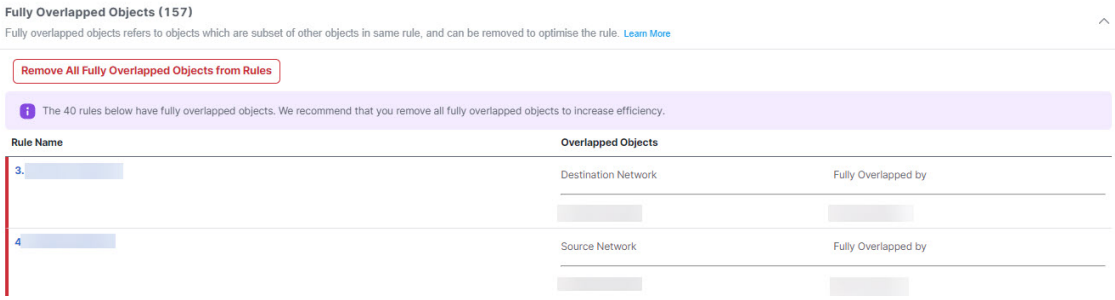
シャドウルールを無効化した後も、変更を適用する前に[元に戻す（Undo）]を選択できます。後でルールを削除すると完全に削除されるため、最初にルールを無効化して影響を測定し、削除することを推奨します。

ルールが存在する クラウド提供型 Firewall Management Center または オンプレミス Firewall Management Center に移動することで、無効になっているルールをいつでも有効にできます。

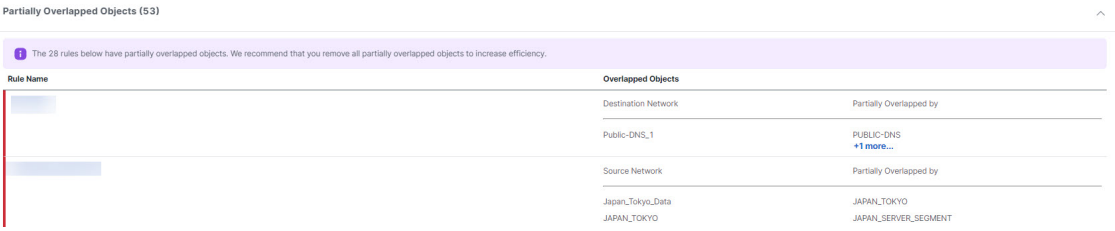
重複するオブジェクト

[重複するオブジェクト（Overlapping Objects）] タブには、完全に重複する（IP アドレスが同じか、完全なサブセットである）オブジェクト、または部分的に重複する（IPアドレスの一部のサブセットが重複しているが、アドレス全体ではない）オブジェクトが一覧表示されます。

たとえば、ルールに 192.168.1.1 のオブジェクトと 192.168.1.0/24 の別のオブジェクトが含まれている場合、192.168.1.1 オブジェクトは他のオブジェクトと完全に重複しているため、ルールに必要ありません。[完全に重複しているすべてのオブジェクトをルールから削除する（Remove All Fully Overlapped Objects from Rules）] ボタンをクリックできます。



部分的な重複の場合は、発生するたびに評価して、変更できるかどうかを判断し、オブジェクトを編集してそれらの変更を直接実装する必要があります。



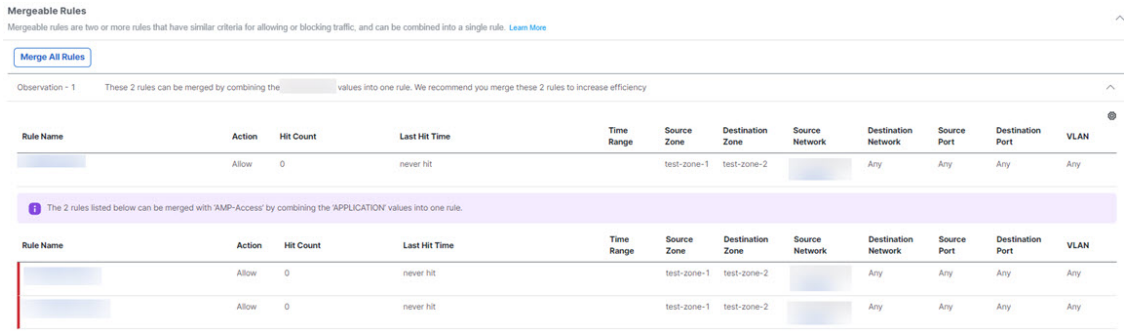
期限切れのルール

[期限切れのルール（Expired Rules）] タブには、時間範囲が期限切れになったルールが一覧表示されます。また、ルールが期限切れになった日付、ヒットカウント、最終ヒット時間、時間範囲などのルール情報を確認できます。

[すべての期限切れルールを無効化（Disable All Expired Rules）] または [すべての期限切れルールを削除（Delete All Expired Rules）] を選択できます。

マージ可能なルール

[マージ可能なルール（Mergeable Rules）] タブには、許可設定とブロック設定が類似していて、1 つのルールにマージできるルールが一覧表示されます。観測内容を読み取り、[すべてのルールをマージ（Merge All Rules）] をクリックして該当するルール内のオブジェクトをマージし、管理するルールの数を削減できます。



（注） 2 つのルールをマージすると、最初のルールのロギング設定が、最初のルールがマージされているルールに適用されるため、マージされたルールのロギング動作は、最初のルールの設定に従い、他のルールの一意のロギング設定はすべて上書きされます。

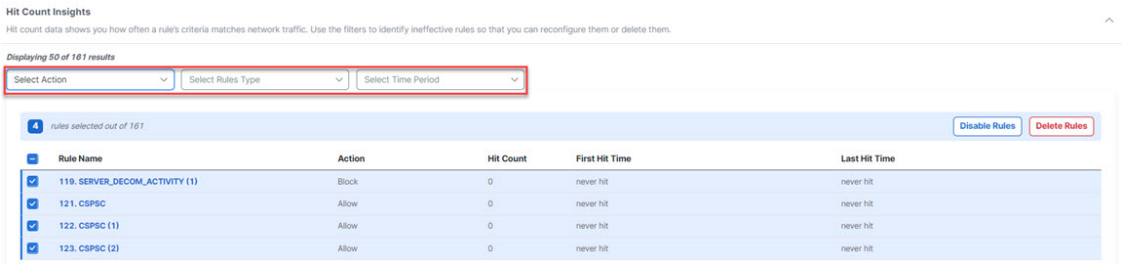
ポリシーインサイト

[ポリシーインサイト（Policy Insights）] タブの [ヒットカウント（Hit Count）] セクションには、トリガーされたことがないルール（[一度もヒットしていないルール（Never Hit Rules）]）が最初に表示されます。ヒットカウント情報は、ポリシーに割り当てられているすべてのデバイスから取得されます。条件を変更したり、他のヒットカウント情報（過去 6 ヵ月間の [ヒットしていないルール（Not Hit Rules）] や、選択した期間の [ヒットしたルール（Hit Rules）] な

ど）を表示したりできます。ルール、ヒット情報、および期間に設定されたアクションを使用して、ルールをフィルタ処理できます。

- [一度もヒットしていないルール（Never Hit Rules）]：作成時から一度もヒットしていないルール。
- [ヒットしたルール（Hit Rules）]：選択した期間にヒットしたルール。
- [ヒットしていないルール（Not Hit Rules）]：選択した期間にヒットしていないルール。

無効化または削除するルールを選択し、[ルールの無効化（Disable Rules）]または[ルールの削除（Delete Rules）]をクリックします。最初にルールを無効化して、無効化の影響を測定してから削除することを推奨します。



ポリシー修復

分析の概要から異常のあるルールを削除または無効化する場合、ポリシーアナライザおよびオプティマイザ ではそれらの変更はすぐに適用されません。必要な変更がステージングされ、[修復の適用（Apply Remediation）]をクリックした場合にのみ適用されます。

[修復の適用（Apply Remediation）]をクリックすると、同じレポートに基づいた修復は再度適用できません。新しいポリシー設定でポリシー分析を再度実行し、新しいレポートを使用して異常を修復する必要があります。

ポリシー修復の適用

始める前に

- 修復を適用する前に、すべてのポリシーのバックアップを作成してください。
- 適用されるようにステージングされたいくつかのポリシー修復があることを確認します。ステージングされた変更がない場合、[修復の適用（Apply Remediation）]ボタンは無効になります。
- 右上隅にある [ポリシーの最終変更日（Policy Last Modified）]、[ポリシーの最終分析日（Policy Last Analyzed）]の日付とタイムスタンプ、および修復対象としてマークしたルールの数を確認することで、修復を適用するポリシーのバージョンを確認できます。

手順

ステップ 1 [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] ページで、[修復の適用（Apply Remediation）] をクリックします。

ステップ 2 適用されるすべての修復の要点を含む確認ポップアップに目を通し、修復しないポリシーに修復を適用していないことを確認します。

ステップ 3 [適用（Apply）] をクリックします。

（注）
[適用（Apply）] をクリックすると、「修復が適用されています（Remediations are being applied）」や「ポリシーは修復のためにロックされています（The policy is locked for remediation）」などのポップアップメッセージが表示されます。

ステップ 4 修復が正常に完了したら、[最適化レポートのダウンロード（Download Optimization Report）] をクリックします。

修復が適用されるとポリシーが変更されるため、新たに変更された一連のポリシーを再分析して別の分析の概要を取得する必要があります。その概要を使用して、残りのポリシーの異常を修復できます。

修復レポートには、適用されたすべての修復および修復が適用されたルールの統合データが含まれています。[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）] ページでポリシーを選択すると、右側のペインに [修復履歴（Remediation History）] が表示されます。履歴には、修復の日時、修復を開始したユーザー、および修復ステータスに関するデータが含まれています。また、同じポップアップから修復レポートをダウンロードできます。

すべての修復が記録され、修復の日時、修復を実行したユーザーなどの情報とともに、[修復履歴（Remediation History）] に表示されます。

（注）
変更管理ワークフローが有効になっている オンプレミス Firewall Management Center の場合、ポリシー修復が適用されると、内部ワークフローチケットが作成され、変更がステージングされます。変更は、チケットが送信または承認された場合にのみ有効になります。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Change Management」を参照してください。

ポリシー修復レポートに含まれる内容

ポリシー修復レポートは、完了した修復部分がすべて統合されており、PDF としてダウンロードできます。このレポートには、ポリシーに対して実行した修復に基づいて、以下のセクションが含まれます。各セクションには、ルール名、実行された修復アクション、および関連するコメントに関する情報が記載されています。たとえば、重複ルールを修復していない場合、レポートには重複ルールの修復に関連するセクションは含まれません。

- 修復の概要

- ヒットカウントの修復
- 期限切れルールの修復
- 重複ルールの修復
- マージ可能なルールの修復

（注） ポリシーが ポリシーアナライザおよびオプティマイザ によって修復されているか確認するには、**[ポリシー（Policies）]**>**[アクセスポリシー（Access Policies）]**に移動し、ポリシーを編集して [ポリシーエディタ（Policy Editor）] でルールを表示します。ポリシーが ポリシーアナライザおよびオプティマイザによって修復されると、最適化されたルールにコメントが追加されます。また、ポリシーアナライザおよびオプティマイザによって最適化されたすべてのルールを「ポリシーアナライザおよびオプティマイザによって更新」を使用してフィルタ処理し、ポリシーアナライザおよびオプティマイザによって修復されたすべてのルールを表示できます。

ポリシーアナライザおよびオプティマイザのトラブルシューティング

ポリシーアナライザおよびオプティマイザに関する問題をトラブルシューティングするには、以下の項を参照してください。

ポリシーアナライザとオプティマイザでポリシーが分析されない

[ポリシーの分析（Analyze Policy）] をクリックしても ポリシーアナライザおよびオプティマイザ でポリシーが分析されない場合は、次の手順を試してください。

手順

ステップ 1 **[管理（Administration）]** > **[Firewall Management Center]**に移動します。

ステップ 2 ポリシー分析が実行されていない オンプレミス Management Center または [クラウド提供型FMC（Cloud-Delivered FMC）] を選択し、右側のペインの [アクション（Actions）] で [ワークフロー（Workflows）] を選択します。

ステップ 3 最新のワークフローの [現在の状態（Current State）] が [エラー（Error）] の場合は、ワークフローを展開し、[終了状態（END STATE）] が [エラー（ERROR）] である最後のアクションまでスクロールします。

ステップ 4 [結果（RESULT ）] 列の下にある [エラーメッセージ（Error Message）] をクリックして詳細なエラーメッセージ確認するか、[スタックトレース（Stack Trace）] をクリックしてエラーの原因となった一連の例外を確認します。

ステップ 5 エラーを解決するか、Cisco TAC に連絡してサポートを受けてください。

ポリシーアナライザとオプティマイザでポリシーが取得されない

オンプレミス Management Center のポリシーが Security Cloud Control の ポリシーアナライザおよびオプティマイザ ページに表示されない場合は、次の手順を実行します。

手順

ステップ 1 オンプレミス Management Center で、**[統合（Integration）] > [Cisco Security Cloud]** に移動します。

ステップ 2 [ポリシーアナライザとオプティマイザの有効化（Enable Policy Analyzer and Optimizer）] 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。

ステップ 3 （任意） Security Cloud Control テナントの左側のナビゲーションウィンドウで、**[ツールとサービス（Tools & Services）] > [Firewall Management Center]** に移動し、オンプレミス Management Center がアクティブで到達可能であることを確認します 。

ポリシーアナライザとオプティマイザに関するよくある質問（FAQ）

ポリシーアナライザおよびオプティマイザを使用して手動で実行する代わりに、Cisco AI Assistant でポリシーを分析して修復できますか。

Cisco AI Assistant は ポリシーアナライザおよびオプティマイザ と連携して、異常のあるポリシーを精査し、ユーザーに通知しますが、人工知能アシスタントはポリシーを自動的に分析して修復することはできません。

ポリシーアナライザおよびオプティマイザは、分析済みのポリシーに対する新たな変更を検出し、同じポリシーで分析を再度実行できますか。

いいえ。 ポリシーアナライザおよびオプティマイザ は、手動でトリガーされた場合、または 24 時間単位でスケジュールされたポリシー分析の実行時にのみポリシーを分析できます。

共有ポリシーの場合、ポリシーアナライザおよびオプティマイザでは個々のデバイスベースのレポートが提供されますか。

いいえ。ポリシーアナライザおよびオプティマイザは、アクセスポリシー分析データに基づいてのみレポートを提供します。

私は オンプレミス Firewall Management Center ユーザーですが、ポリシーアナライザおよびオプティマイザ を使用するには、Security Cloud Control 基本ライセンスを購入する必要がありますか。

いいえ。ポリシーアナライザおよびオプティマイザ は、Cisco Security Cloud の統合時に既存または新たに作成された Security Cloud Control テナントの一部として提供されます。

オンプレミス Firewall Management Center を Cisco Security Cloud と統合したときに Security Cloud Control テナントをプロビジョニングしましたが、ポリシーアナライザおよびオプティマイザ以外に Security Cloud Control で活用できる機能はどれか。

この Security Cloud Control テナントの ポリシーアナライザおよびオプティマイザ 機能のみ活用できます。Security Cloud Control の他の機能を使用するには、Security Cloud Control 基本ライセンスとその他のデバイス固有のライセンスを購入する必要があります。

オンプレミス Firewall Management Center で変更管理ワークフローが有効になっており、承認待ちの変更があるポリシーがある場合、ポリシーアナライザおよびオプティマイザはそれらのポリシーを修復できますか。

いいえ。ポリシーは使用目的でロックされているというエラーが表示され、修復されません。

ポリシーアナライザおよびオプティマイザが1つのポリシーで分析できるルールに最大数はありますか。

最大数の制限はありません。ポリシーアナライザおよびオプティマイザ は、任意の数のポリシーとルールを分析できますが、ルール数が多いポリシーの場合、分析にも時間がかかります。

ルールの無効化とルールの削除の違いは何ですか。どちらが良いオプションですか。

ルールを削除すると、そのルールはデバイスのメモリから完全に削除されますが、無効にした場合、ルールはバックアップとしてデバイスのメモリに保持され、デバイスに展開されません。

部分的に完了しているポリシーの修復が失敗した場合、変更はポリシーアナライザおよびオプティマイザ によって自動的に取り消されますか。

いいえ。そのような場合、障害通知と修復レポートが表示されます。レポートを読んで、不完全な修復の影響を受けたルールを確認し、変更を手動で取り消して、修復を最初からやり直すことができます。

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。