アクセス制御ポリシー

ここでは、アクセス コントロール ポリシーの使用して作業する方法について説明します。

アクセス コントロール ポリシーについて

アクセス制御は、ネットワーク トラフィックの指定、検査、ロギングが可能な階層型ポリシーです。各接続の特性を使用して、接続を許可、信頼、ブロック、または監視できます。

各管理対象デバイスは、1つのアクセス コントロール ポリシーに割り当てることができます。ポリシーが割り当てられたデバイス（ターゲット デバイスとも）がネットワーク トラフィックについて収集したデータは、以下に基づいてそのトラフィックのフィルタや制御に使用できます。

- トランスポート層およびネットワーク層の特定しやすい単純な特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- レルム、ユーザ、ユーザ グループ、または ISE の属性
- カスタム セキュリティ グループ タグ（SGT）
- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入の試みが存在するかどうか
- 時刻と日（サポートされているデバイス上）

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーションベースのブロッキングはシンプルな送信元と宛先のデータを使用しているため、禁止されているトラフィックを初期の段階でブロックできます。これに対し、侵入およびエクスプロイトの検知とブロックは最終防衛ラインです。

アクセス コントロール ポリシーのコンポーネント

アクセス コントロール ポリシーの主な要素は次のとおりです。

名前と説明

各アクセス コントロール ポリシーには一意の名前が必要です。説明は任意です。

継承設定

ポリシー継承により、アクセス コントロール ポリシーの階層を作成することができます。親（または基本）ポリシーは子孫のデフォルト設定を定義、実行します。

ポリシーの継承設定で基本ポリシーを選択できます。また、現在のポリシーで設定をロックすることで、子孫にも同じ設定を継承させることできます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

ポリシーの割り当て

各アクセス コントロール ポリシーがそのポリシーを使用するデバイスを識別します。それぞれのデバイスは、1 つのアクセス コントロール ポリシーのみのターゲットに設定できます。デバイステンプレートにポリシーを割り当てることもできます。

ルール（Rule）

アクセス コントロール ルールは、ネットワーク トラフィックをきめ細かく処理する方法を提供します。先祖ポリシーから継承したルールを含むアクセス コントロール ポリシーのルールには、1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、アクセス コントロール ルールをトラフィックと照合します。

通常、システムは、ルールのすべての条件がトラフィックに一致する最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。条件は単純または複雑にできます。条件の使用は特定のライセンスによって異なります。

デフォルトアクション

デフォルト アクションは、他のアクセス制御設定で処理されないトラフィックをどのように処理し、ロギングするかを定義します。デフォルト アクションにより、追加のインスペクションなしですべてのトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリ データの有無についてトラフィックを検査することもできます。

アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

セキュリティ インテリジェンス（Security Intelligence）

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防衛ラインです。この機能により、最新の IP アドレス、URL、ドメイン名レピュテーションインテリジェンスをもとに接続をブロックすることができます。重要なリソースへの継続的なアクセスを確保するために、ブロックリストのエントリはカスタムブロックしないリストのエントリで上書きできます。

HTTP応答数

システムによりユーザの Web サイト リクエストがブロックされた場合、システム提供の汎用的な応答ページを表示するか、カスタム ページを表示させることができます。ユーザーに警告するページを表示するものの、ユーザーが最初に要求したサイトに進めるようにすることもできます。

ログ

アクセス コントロール ポリシー ロギングの設定を使用して、現在のアクセス コントロール ポリシーのデフォルトの syslog の宛先を設定できます。この設定は、syslog の宛先設定が組み込まれているルールとポリシーのカスタム設定で明示的にオーバーライドされない限り、アクセス コントロール ポリシーと組み込まれているすべての復号、プレフィルタ、および侵入ポリシーに適用されます。

高度なアクセス制御オプション

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。多くの場合、デフォルト設定が適切です。詳細設定では、トラフィックの前処理、復号、ID、種々のパフォーマンス オプションなどを変更できます。

アクセス コントロール ポリシーのデフォルト アクション

新しく作成したアクセス コントロール ポリシーは、デフォルト アクションを使用して、すべてのトラフィックを処理するようにターゲット デバイスに指示します。

単純なアクセス コントロール ポリシーでは、デフォルト アクションは、ターゲット デバイスがすべてのトラフィックをどう処理するかを指定します。より複雑なポリシーでは、デフォルト アクションは次のトラフィックを処理します。

- プリフィルタ ポリシーによって高速パス処理されない
- セキュリティ インテリジェンス ブロック リストにないトラフィック
- 復号ポリシーによってブロックされない（暗号化トラフィックのみ）
- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

アクセス コントロール ポリシーのデフォルト アクションにより、追加のインスペクションなしでトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリ データの有無についてトラフィックを検査することもできます。

（注） デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。デフォルトアクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。

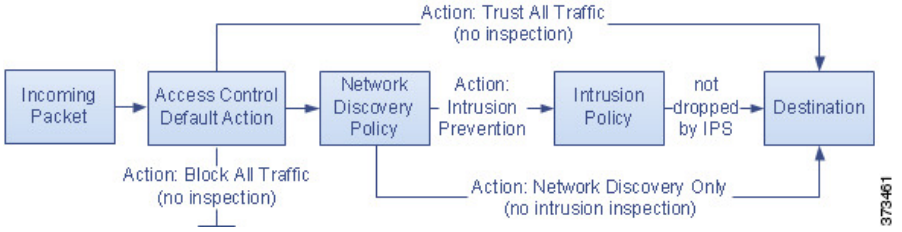
ポリシーを継承している場合、最下位の子孫のデフォルトアクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは基本ポリシーから継承することもできますが、継承したデフォルトアクションを強制的に実施することはできません。

次の表に各デフォルトアクションが処理するトラフィックに対して実施可能なインスペクションの種類を示します。

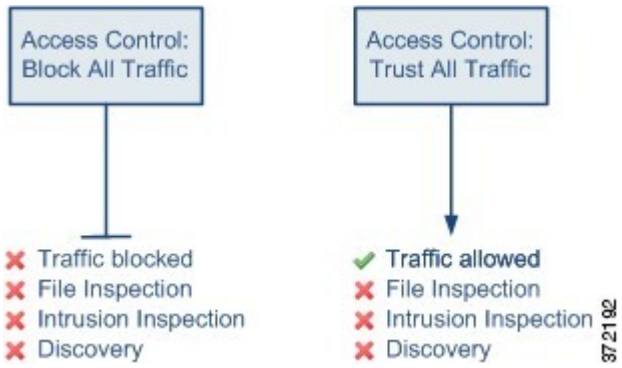
表 *1:* アクセス コントロール ポリシーのデフォルト アクション

デフォルト アクション	トラフィックに対して行う処理	インスペクション タイプとポリシー
アクセス コントロール：すべてのトラフィックをブロック	それ以上のインスペクションは行わずにブロックする	なし。
アクセス コントロール：すべてのトラフィックを信頼	信頼（追加のインスペクションなしで最終宛先に許可）	なし。
侵入防御	ユーザーが指定した侵入ポリシーに合格する限り、許可する	侵入、指定した侵入ポリシーおよび関連する変数セットを使用 検出（discovery）、ネットワーク検出ポリシーを使用
ネットワーク検知のみ	許可。	検出のみ、ネットワーク検出ポリシーを使用。
ベースポリシーからの継承	基本ポリシーで定義。	基本ポリシーで定義。

次の図は、表を図で表したものです。



次の図は、[すべてのトラフィックをブロック（Block All Traffic）]および[すべてのトラフィックを信頼（Trust All Traffic）] のデフォルト アクションを示しています。



次の図は、[侵入防御（Intrusion Prevention）] および [ネットワーク検出のみ（Network Discovery Only）] のデフォルト アクションを説明しています。

ヒント [ネットワーク検出のみ（Network Discovery Only）] の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入検知および防御のみを目的としている場合は、さまざまな設定でディスカバリを無効にできます。

アクセス コントロール ポリシーの継承

アクセス コントロール ポリシーはネストすることができます。このポリシーでは各ポリシーが先祖（または基本）ポリシーからルールや設定を継承します。この継承を強制することもできますが、下位のポリシーによる先祖ポリシーの上書きを許可することもできます。

アクセス制御は階層型ポリシーベース実装となっています。ドメイン階層を作成するのと同様に、対応するアクセス コントロール ポリシーの階層を作成できます。子孫（あるいは子）アクセス コントロール ポリシーは、直接の親（あるいは基本）ポリシーからルールや設定を継承します。この基本ポリシーにもさらに親ポリシーがあり、その親ポリシーにもさらに、というようにルールや設定が継承されている場合もあります。

アクセス コントロール ポリシーのルールは、親ポリシーの [強制（Mandatory）] ルール セクションと [デフォルト（Default）] のルール セクションの間にネストされています。この実装により、先祖ポリシーの [強制（Mandatory）] ルールは実施される一方、先祖ポリシーの [デフォルト（Default）] ルールは現在のポリシーでプリエンプション処理することが可能です。

次の設定をロックすることで、すべての子孫ポリシーに設定を実行させることができます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

- セキュリティインテリジェンス：IPアドレス、URL、ドメイン名の最新のレピュテーション インテリジェンスをもとに接続を許可またはブロックされた接続。
- HTTP 応答ページ：ユーザーの Web サイト リクエストをブロックした際、カスタム応答ページあるいはシステム提供の応答ページを表示します。
- 詳細設定：関連するサブポリシー、ネットワーク分析設定、パフォーマンス設定、その他の一般設定オプションを指定します。

ポリシーを継承している場合、最下位の子孫のデフォルトアクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

ポリシーの継承とマルチテナンシー

アクセス コントロールの階層型ポリシーベース実装はマルチテナンシーを補完します。

通常のマルチドメイン導入環境では、アクセス コントロール ポリシーの階層がドメイン構造に対応しており、管理対象デバイスに最下位レベルのアクセス コントロール ポリシーを適用します。この実装により、ドメインの上層レベルでは選択的にアクセス制御を実施しながらも、ドメインの下層レベルの管理者は展開ごとに設定を調整することが可能です（子孫ドメインの管理者を制限するには、ポリシー継承と適用だけでなく、ロールによる制限を行う必要があります）。

たとえば、所属している部門のグローバル ドメイン管理者は、グローバル レベルのアクセス コントロール ポリシーを作成できます。そして、そのグローバル レベルのポリシーを基本ポリシーとして、機能別にサブドメインに分けられたすべてのデバイスで使用するよう要求することがことが可能です。

サブドメインの管理者が Secure Firewall Management Center にログインしてアクセス制御を設定する際、グローバル レベルのポリシーはそのまま展開できます。あるいは、グローバル レベルのポリシーの範囲内の子孫アクセス コントロール ポリシーを作成、展開することも可能です。

（注） アクセス制御の継承および適用が最も有効に実装されるのは、マルチテナンシーを補完する場合ですが、1 つのドメイン内においてもアクセス制御ポリシーを階層化することが可能です。また、任意のレベルでアクセス コントロール ポリシーを割り当て、展開することもできます。

ルールおよび他のポリシー警告

ポリシーおよびルールエディタでは、トラフィックの分析やフローに悪影響を与える可能性のある設定をアイコンで示します。問題に応じて、システムはユーザがそのようなポリシーを展開しようとするときに警告するか、導入を完全に阻止します。

ヒント　警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。

表 *2:* ポリシーのエラー アイコン

アイコン	説明	例
Errors ( )	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまではポリシーを展開できません。	カテゴリおよびレピュテーション ベースのURLフィルタリングを実行するルールは、URLフィルタリング ライセンスのないデバイスを割り当てる時点まで有効です。その時点で、ルールの横にエラー アイコンが表示され、ポリシーを展開できなくなります。ポリシーを展開するには、このルールを編集または削除するか、デバイスの割り当て解除をするか、URL フィルタリング ライセンスを有効にする必要があります。
Warning ( )	ルールに関する警告またはその他の警告が表示されていても、ポリシーを展開することはできます。しかし、警告でマークされている誤った設定は有効になりません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。	プリエンプトされるルール、または誤った設定によりトラフィックを照合できないルールは有効になりません。誤った設定には、空のオブジェクト グループ、一致するアプリケーションがないアプリケーション フィルタ、除外された LDAP ユーザ、無効なポートなどを使用した条件が含まれます。 一方、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題を修正するまでそのポリシーを展開することはできません。
Information ( )	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題によってポリシーの展開が阻止されることはありません。	システムは接続でアプリケーション トラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあります。これにより、アプリケーションと HTTP 要求が識別されるように接続が確立されます。

アイコン	説明	例
Rule Conflict (〜)	ルール競合分析を有効にすると、競合のあるルールのルールテーブルにこのアイコンが表示されます。	競合には、冗長なルール、冗長なオブジェクト、およびシャドウイングされたルールが含まれます。以前のルールがすでに基準に一致しているため、冗長なルールやシャドウイングされたルールはトラフィックと一致しません。冗長なオブジェクトは、ルールを不必要に複雑にします。

アクセス コントロール ポリシーの要件と前提条件

Model support

任意

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin
- カスタムユーザーロールを定義して、アクセス コントロール ポリシーおよびルールの侵入設定と、その他のアクセス コントロール ポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、すべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。詳細な権限は次のとおりです。
  - **Policies** > **Access Control heading** > **Access Control[アクセスコントロールポリシー（Access Control Policy）]** > **[アクセスコントロールポリシーの変更（Modify Access Control Policy）]** > **[脅威設定の変更（Modify Threat Configuration）]**では、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、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 ポリシーの構成、およびポリシーのデフォルト アクションの侵入アクションの選択を行えます。これ以外のオプションが表示されない場合、ユーザーはポリシーまたはルールの他の部分を変更できません。
  - [残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] は、ポリシーの他のすべての側面を編集する機能を制御します。

アクセス コントロール ポリシーの管理

システム付属のアクセス コントロール ポリシーの編集と、カスタム アクセス コントロール ポリシーの作成が可能です。

手順

ステップ 1 **Policies** > **Access Control heading** > **Access Control**を選択します。

ページの上部には、オブジェクト管理、侵入ポリシー、ネットワーク分析ポリシー、DNS ポリシー、ポリシーのインポート/エクスポートなどの関連機能への便利なリンクがあります。

ステップ 2 アクセス コントロール ポリシーを管理します。

- ポリシーの分析：1 つ以上のポリシーを選択して **[ポリシーの分析（Analyze Policies）]** をクリックすることで、冗長ルールやシャドウルールなどの異常に対するアクセス コントロール ポリシーを評価し、検出された異常を修正するアクションを実行できます。分析ジョブはクラウドに送信され、完了までに時間がかかります。「ポリシーアナライザとオプティマイザを使用した異常の特定と修正 （23 ページ）」を参照してください。

  [異常（Anomalies）]列に分析の結果が表示されます。[最適化可能な割合（% Optimizable）] リンクをクリックして異常を表示するか、[再分析（Re-Analyze）] をクリックして分析を再実行します。[最後の分析（Last Analyzed）]列には、ポリシーアナライザおよびオプティマイザが最後に実行された日時が表示されます。

  分析と最適化が完了したら、**More** (⋮) メニューから [最後のポリシー分析のダウンロード（Download Last Policy Analysis）] > [修復履歴（Remediation History）] のオプションを選択して、レポートをダウンロードできます。

  （注）
  ポリシー分析機能を使用するには、Cloud-Delivered Firewall Management Center または を Security Cloud Control（Security Cloud Control）に接続する必要があります。設定が要件を満たしていない場合は、このボタンをクリックすると開く説明ダイアログに [統合（Integrate）]ボタンが含まれており、開始することができます。ポリシーアナライザとオプティマイザはクラウドでのみ動作します。

- 作成：**[新規ポリシー（New Policy）]** をクリックします。基本的なアクセス コントロール ポリシーの作成 （10 ページ） を参照してください。

- [列（Columns）]：ルールのリストの上にある [列の表示/非表示（Show/Hide Columns）] アイコンをクリックして、テーブルに表示する情報を選択します。[[すべて表示（Show All）]/[すべて非表示（Hide All）] をクリックすると、名前とアクションを除き、リストされているすべての列をすばやく追加または削除できます。すべてのカスタマイズを元に戻すには、[デフォルト（Default）] をクリックします。

- [継承（Inheritance）]：継承：子孫を持つポリシーの横にある**プラス**をクリックすると、ポリシーの階層ビューが展開されます。
- 編集：**Edit** (✎)をクリックします。アクセス コントロール ポリシーの編集 （11 ページ）を参照してください
- 削除：**Delete** (🗑) をクリックします。ポリシーを削除する前に、デバイスの割り当てを削除する必要があります。

  一度に複数のポリシーを削除するには、ポリシーのチェックボックスをオンにし、テーブルの上にある [ポリシーの削除（Delete Policies）] を選択します。
- [コピー（Copy ）]：**More** (⋮) メニューから [複製（Clone）] を選択します。デバイスの割り当てはコピーに保持されません。
- [レポート（Report）]： **More** (⋮)メニューから **[レポートの生成（Generate Report）]** を選択しますをクリックします。. レポートは、バックグラウンド プロセスとして生成されます。メッセージ/通知センターに移動し、タスク リストを調べます。レポートが完了したら、通知からダウンロードできます。
- 監査ログの表示：**More** (⋮) から **[監査ログへ移動（Go to Audit Log）]** をクリックします。
- ポリシーのロックまたはロック解除：アクセス コントロール ポリシーのロック （14 ページ）を参照してください。

基本的なアクセス コントロール ポリシーの作成

新しいアクセス コントロール ポリシーを作成すると、そのポリシーにデフォルトのアクションと設定が含まれます。ポリシーを作成すると、要件に合わせてポリシーを調整できるよう、すぐに編集セッションに移行します。

手順

ステップ 1 **Policies** > **Access Control heading** > **Access Control** を選択します。

ステップ 2 **、[新しいポリシー（New Policy）]** の順にクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 必要に応じて、基本のポリシーを選択します。

ドメインにアクセス コントロール ポリシーが適用されている場合は、この手順はオプションではありません。適用されているポリシーまたはその子孫のいずれかを基本ポリシーとして選択する必要があります。

基本ポリシーを選択すると、基本ポリシーによってデフォルトアクションが定義されるため、このダイアログボックスで新しいアクションを選択することはできません。デフォルトアクションによって処理される接続のロギングは、基本ポリシーによって異なります。

ステップ 5 基本ポリシーを選択しない場合は、初期の**デフォルトアクション**を指定します。

- [すべてのトラフィックをブロック（Block All Traffic）] を選択すると、[アクセス コントロール：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をデフォルト アクションとするポリシーが作成されます。
- [侵入防御（Intrusion Prevention）] を選択すると、[侵入防御：セキュリティと接続性のバランス（Intrusion Prevention: Balanced Security and Connectivity）] をデフォルト アクションとし、デフォルトの侵入変数セットが関連付けられたポリシーが作成されます。
- [ネットワーク検出（Network Discovery）] を選択すると、[ネットワーク検出のみ（Network Discovery Only）] をデフォルト アクションとするポリシーが作成されます。

デフォルトアクションを選択した場合、デフォルトアクションで処理される接続のロギングは、最初は無効になっています。この設定は、後でポリシーを編集するときに有効にできます。

ヒント
デフォルトですべてのトラフィックを信頼するか、基本ポリシーを選択しデフォルトアクションは継承しないようにする場合は、後でデフォルト アクションを変更できます。

ステップ 6 オプションで、ポリシーを割り当てるデバイスを選択します。表示されるデバイスを絞り込むには、検索文字列を入力します。このリストには、デバイスとデバイステンプレートの両方が含まれています。

このポリシーをすぐに展開するには、この手順を実行する必要があります。

ステップ 7 [保存（Save）] をクリックします。

新しいポリシーが開いて編集できる状態になります。必要に応じてルールを追加したり、その他の変更を加えたりすることが可能です。アクセス コントロール ポリシーの編集 （11 ページ）を参照してください。

アクセス コントロール ポリシーの編集

アクセス コントロール ポリシーを編集するときは、そのポリシーをロックして、同時に編集する可能性がある別のユーザーによって変更が上書きされないようにする必要があります。

現在のドメインで作成されたアクセス コントロール ポリシーのみ編集できます。また、先祖アクセス コントロール ポリシーによってロックされている設定は編集できません。

セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

（注） ポリシーをロックしない場合、次を検討します：1 つのブラウザウィンドウを使用して、一度に 1 人のみで行う。一度に複数のユーザーがアクセス コントロール ポリシーを編集できても、1 人のユーザーが、変更をほぞんしたら、別のユーザーが行ったすべての変更は、即座に削除され、これらのユーザーの編集モードが解除され、アクセス コントロール ポリシー一覧ページに戻ります。これらの別のユーザーは、最初から変更しなおす必要があります。

手順

ステップ 1 **Policies** > **Access Control heading** > **Access Control**を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある **Edit** (✎) をクリックします。

代わりに **View** (👁) 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 アクセス コントロール ポリシーを編集します。

ヒント
左列でチェックボックスを選択し、検索ボックスの横にある **[一括ルールアクションを選択（Select Bulk Rule Actions）]** ドロップダウンリストから実行するアクションを選択すると、一度に複数のルールを操作できます。ルールの有効化と無効化、コピー、移動、削除、編集、またはヒットカウントや関連イベントの表示には、一括編集を使用できます。選択したルール内のオブジェクトの重複を削除することもできます。

次のような設定の変更やアクションの実行が可能です。

- 名前と説明：名前の横の **Edit** (✎) をクリックして変更を加え、**[保存（Save）]** をクリックします。
- デフォルトのアクションと設定：**[デフォルト アクション（Default Action）]** ドロップ ダウンリストから値を選択し、 **Cog** (⚙) をクリックして設定を変更し、**[OK]**をクリックします。詳細については、アクセス コントロールのデフォルト アクションを設定 （15 ページ）を参照してください。
- 関連付けられたポリシー：パケットフローのポリシーを編集または変更するには、ポリシー名の下のパケットフロー表示でポリシータイプをクリックします。[プレフィルタルール（Prefilter Rules）]、**[復号（Decryption）]**、[セキュリティインテリジェンス（Security Intelligence）]、および [ID（Identity）] ポリシーを選択できます。必要に応じて、[アクセス制御（Access Control）] をクリックしてアクセスコントロールルールに戻ります。
- ポリシー割り当て：このポリシーの対象となる管理対象デバイスを特定するか、このポリシーをサブドメインに適用するには、**ターゲットされた: x デバイス** リンクをクリックします。デバイスまたはデバイステンプレートにポリシーを割り当てることができます。
- ルール：アクセスコントロールルールを管理し、侵入ポリシーとファイルポリシーを使用して悪意のあるトラフィックを検査およびブロックするには、[ルールの追加（Add Rule）]

をクリックするか、既存のルールを右クリックして [編集（Edit）] またはその他の該当するアクションを選択します。アクションは、各ルールの **More** (⋮) ボタンからも選択できます。アクセス コントロール ルールの作成および編集を参照してください。

- レイアウト：ルールのリストの上にある [グリッド/テーブルビュー（Grid/Table View）] アイコンを使用して、レイアウトを変更します。グリッドビューでは、色分けされたオブジェクトが見やすいレイアウトで表示されます。テーブルビューでは、一度に複数のルールを確認できるように概要リストが表示されます。ビューは、ルールに影響を与えることなく自由に切り替えることができます。
- 列（テーブル ビューのみ）：ルールのリストの上にある [列の表示/非表示（Show/Hide Columns）] アイコンをクリックして、テーブルに表示する情報を選択します。情報がない（どのルールでもそれらの条件を使用していない）すべての列をすばやく追加、または削除するには、**[空の列を表示/非表示（Hide Empty Columns）]** をクリックします。すべてのカスタマイズを元に戻すには、[デフォルトに戻す（Revert to Default）] をクリックします。
- 分析ルールのロジック：**[分析（Analyze）]** メニューから次のオプションを選択して、ルールのロジックを調べることができます。
  - **管理ルール ヒット カウント**：各ルールに一致した接続の数に関する統計を表示します。ルール ヒット カウントの表示 （24 ページ）を参照してください。
  - [ルールの競合を有効/無効にする（Enable/Disable Rule Conflicts）]：ルールが互いに干渉するかどうかに関する情報の表示/非表示を切り替えます。その後、次のコマンドを使用して結果を表示できます。「ルールの競合および警告の分析 （27 ページ）」を参照してください。
    - **警告およびエラーを表示**：対処する必要がある構成の問題を含むルールがあるかどうかを表示します。
    - **ポリシー警告の表示**：ポリシーの設定上の問題があるかどうかを確認します。
    - [ルール競合の表示（Show Rule Conflicts）]：冗長ルールまたはシャドウイングされたルールがあるかどうかを表示します。この競合により、特定のルールが接続に一致しなくなる可能性があります。そのため、一致基準の修正、ルールの移動、またはルールの削除が必要になります。
- 追加設定：ポリシーの追加設定を変更するには、パケットフロー行の最後にある **[詳細（More）]** ドロップダウン矢印から次のオプションのいずれかを選択します。
  - **詳細設定**：前処理、復号、アイデンティティ、パフォーマンス、およびその他の詳細オプションを設定します。アクセス コントロール ポリシーの詳細設定の構成を参照してください。
  - HTTP レスポンス：システムが Web サイトの要求をブロックするときにブラウザに表示される情報を指定します。HTTP 応答ページの選択を参照してください。
  - 継承設定：このポリシーの基本アクセス コントロール ポリシーを変更し、このポリシーの設定をその子孫ポリシーに適用します。基本アクセス コントロール ポリシー

の選択 （17 ページ）および子孫アクセス コントロール ポリシーでの設定のロック （18 ページ）を参照してください。

- ロギング：ポリシーのデフォルトのロギングオプションを設定します。

ステップ 4 **[保存（Save）]** をクリックします。

アクセス コントロール ポリシーのロック

アクセス コントロール ポリシーをロックして、他の管理者が編集できないようにすることができます。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。ロックしない場合、複数の管理者がポリシーを同時に編集すると、最初に変更を保存したユーザーによって、他のすべてのユーザーが行った変更が消去されます。

ロックはアクセス コントロール ポリシー自体を目的としています。ポリシーで使用されるオブジェクトにはロックは適用されません。たとえば、ロックされたアクセス コントロール ポリシーで使用されるネットワークオブジェクトを別のユーザーが編集できます。ロックはポリシーを明示的にロック解除するまでそのままなので、ログアウトして後で編集に戻ることができます。

ロックすると、他の管理者にはポリシーへの読み取り専用アクセス権が付与されます。ただし、他の管理者は、ロックされたポリシーを管理対象デバイスに割り当てることができます。

始める前に

アクセスコントロールポリシーを変更する権限を持つすべてのユーザーロールには、ポリシーをロックしたり、別のユーザーによってロックされたポリシーをロック解除したりする権限があります。

ただし、別の管理者によってロックされているポリシーのロックを解除する権限は、**Policies** > **Access Control heading** > **Access Control** の権限によって制御される必要があります。そして、**[アクセス コントロール ポリシー（Access Control Policy）]** > **[アクセス コントロール ポリシーを変更（Modify Access Control Policy）]** > **[アクセス コントロール ポリシー ロックをオーバーライド（Override Access Control Policy Lock）]** の順に選択します。

カスタムロールを使用している場合、組織がこの権限を割り当てないことで、ロック解除権限が制限されている可能性があります。この権限がないと、ポリシーをロックした管理者のみがロックを解除できます。

手順

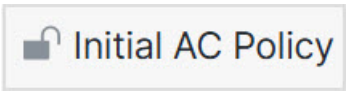
ステップ 1 **Policies** > **Access Control heading** > **Access Control**を選択します。

ステップ 2 ロックまたはロック解除するアクセス コントロール ポリシーの横にある **Edit** (✎) をクリックします。

アクセス コントロール ポリシー リストで、次のようにします。

- ポリシー名の横にあるロックアイコンは、そのポリシーがロックされていることを示しています。ポリシーをロックしたユーザーを確認するには、アイコンにカーソルを合わせます。
- 代わりに **View** () 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。 または、別のユーザーによってロックされています。

ステップ 3 ポリシー名の横にあるロックアイコンをクリックして、ポリシーをロックまたはロック解除します。



ポリシーが親ポリシーから設定を継承する場合、ロックアイコンをクリックしたときに次のオプションのいずれかを選択する必要があります。

- **[このポリシーのロック/ロック解除（Lock/Unlock This Policy）]**：ロックまたはロック解除は、このポリシーのみが対象となります。
- **[階層内のすべてのポリシーのロック/ロック解除（Lock/Unlock all policies in hierarchy）]**：このポリシーとすべての親ポリシーがロックまたはロック解除されます。親ポリシーが別の管理者によって既にロックされている場合、メッセージが表示され、その親ポリシーをロックすることはできません。ポリシーのロックを解除するときに、アクセス コントロール ポリシー ロックのオーバーライド権限を持っている場合、他のユーザーによってロックされていても、すべての親ポリシーがロック解除されます。

アクセス コントロールのデフォルト アクションを設定

アクセス コントロール ポリシーのデフォルトアクションは、次の接続に適用されます。

- プリフィルタ ポリシーによって高速パス処理されない
- セキュリティ インテリジェンス ブロック リストにないトラフィック
- 復号ポリシーによってブロックされない（暗号化トラフィックのみ）
- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

手順

ステップ 1 変更する継承設定を持つアクセス コントロール ポリシーを編集します。アクセス コントロール ポリシーの編集 （11 ページ）を参照してください。

ステップ 2 ルールリストの下部にある **[Default Action]** を選択。

各オプションの機能の詳細については、アクセス コントロール ポリシーのデフォルト アクション （3 ページ） を参照してください。

ステップ 3 **Cog** (⚙) をクリックして、デフォルトのアクションを設定します。

次のオプションを構成します。完了したら、[OK] をクリックします。

- [ロギングオプション（Logging options）]：接続をログに記録するかどうか。 **接続の開始時にロギング**、**接続の終了時にロギング**、またはその両方を行うことができます。デフォルトのアクションとしてブロックを選択した場合は、接続の開始時にのみロギングできます。
- **[接続イベントの送信先（Send connection events to）]**：いずれかのロギング オプションを選択した場合は、次のいずれかの組み合わせにイベントを送信するかどうかを選択します。
  - **ファイアウォール Management Center**：イベントをマネージャに送信します。
  - **Syslog サーバー**：ポリシーに設定されているデフォルトのSyslog サーバーにイベントを送信します。オーバーライドを設定して、別のシビラティ）レベルまたは syslog サーバーの接続先を指定できます。
- **SNMP トラップ**：ロギングを有効にすると、SNMP トラップを SNMP サーバーに送信できます。SNMP 設定を選択か、 **[+]** をクリックして新しい設定を行います。
- **[デフォルトアクションの変数セット（Default action variable set）]**：侵入防御のデフォルトアクションのいずれかを選択した場合、選択した侵入ポリシーで使用される変数セットを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

アクセス コントロール ポリシーの継承の管理

継承は、アクセス コントロール ポリシーの基本ポリシーとして別のポリシーを使用することに関連します。これにより、1 つのポリシーを使用して、複数のポリシーに適用できるいくつかのベースライン特性を定義できます。継承がどのように機能するのかについては、アクセス コントロール ポリシーの継承 （5 ページ） を参照してください。

手順

ステップ 1 変更する継承設定を持つアクセス コントロール ポリシーを編集します。アクセス コントロール ポリシーの編集 （11 ページ）を参照してください。

ステップ 2 ポリシーの継承を管理します。

- 基本ポリシーの変更：このポリシーの基本アクセス コントロール ポリシーを変更するには、パケットフロー行の最後にある **[詳細（More）]** ドロップダウン矢印から **[継承設定（Inheritance Settings）]** を選択し、基本アクセス コントロール ポリシーの選択 （17 ページ） で説明する手順を実行します。
- 子孫の設定のロック：このポリシーの設定を子孫ポリシーで強制適用するには、パケットフロー行の最後にある **[詳細（More）]** ドロップダウン矢印から **[継承設定（Inheritance Settings）]** を選択し、子孫アクセス コントロール ポリシーでの設定のロック （18 ページ） で説明する手順を実行します。
- 基本ポリシーからの設定の継承：基本アクセス コントロール ポリシーから設定を継承するには、基本ポリシーからのアクセス コントロール ポリシー設定の継承 （18 ページ） で説明する手順を実行します。
- ドメインで必須にする：このポリシーをサブドメインで強制適用するには、**[対象：x のデバイス（Targeted: x devices）]** リンクをクリックし、ドメインでのアクセス コントロール ポリシーの強制 （19 ページ） で説明する手順を実行します。

基本アクセス コントロール ポリシーの選択

1 つのアクセス コントロール ポリシーを別の基本（親）として使用できます。デフォルトでは、子のポリシーが基本ポリシーから設定を継承します。ロック解除された設定を変更することも可能です。

既存のアクセス コントロール ポリシーの基本ポリシーを変更すると、システムで現在のポリシー設定が新しい基本ポリシーの任意のロックされた設定に更新されます。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [継承設定（Inheritance Settings）] を選択します。

ステップ 2 [基本ポリシーの選択（Select Base Policy）] ドロップダウンリストからポリシーを選択します。

継承を削除するには、**[なし（None）]** を選択します。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

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。

子孫アクセス コントロール ポリシーでの設定のロック

アクセス コントロール ポリシーの設定をロックして、すべての子孫ポリシーで設定を適用します。子孫ポリシーでは、ロックされていない設定をオーバーライドできます。

設定をロックするときに、すでに子孫ポリシーで実行されていたオーバーライドを保存して、設定のロックを再度解除したときにオーバーライドを復元できるようにします。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [継承設定（Inheritance Settings）] を選択します。

ステップ 2 [子ポリシーの継承設定（Child Policy Inheritance Settings）] 領域で、ロックする設定をオンにします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 [OK] をクリックして継承設定を保存します。

ステップ 4 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

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。

基本ポリシーからのアクセス コントロール ポリシー設定の継承

新しい子ポリシーは、基本ポリシーから多数の設定を継承します。これらの設定は、基本ポリシーでロックされていない場合はオーバーライドできます。

基本ポリシーから後で設定を再継承すると、システムによって基本ポリシーの設定が表示され、コントロールが淡色表示されます。ただし、オーバーライドした内容はシステムによって保存され、その内容は継承を再度無効にすると復元されます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、**[セキュリティ インテリジェンス（Security Intelligence）]** をクリックするか、パケットフロー行の最後にある **[詳細（More）]** ドロップダウン矢印から **[HTTP応答（HTTP Responses）]**、**[ロギング（Logging）]**、**[Encrypted Visibility Engine]**、または **[詳細設定（Advanced Settings）]** を選択します。

ステップ 2 継承する設定ごとに、**[基本ポリシーから継承（Inherit from *(base policy)*）]** チェックボックスをオンにします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 **[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。

ドメインでのアクセス コントロール ポリシーの強制

ドメイン内の各デバイスが同一の基本アクセス コントロール ポリシーまたは、そのポリシーの子孫ポリシーの1つを使用するように強制できます。この手順は、マルチドメイン展開のみに関連するものです。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、**[ターゲット：x デバイス（Targeted: x devices）]** リンクをクリックします。

ステップ 2 [ドメインに強制（Required on Domains）] をクリックします。

ステップ 3 ドメイン リストを作成します。

- 追加：現在のアクセス コントロール ポリシーを強制適用するドメインを選択して [追加（Add）] をクリックするか、選択したドメインのリストにドラッグ アンド ドロップします。
- 削除：リーフドメインの横にある **Delete** ( ) をクリックするか、先祖ドメインを右クリックして [選択項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。検索をクリアするには、**Clear** ( ) をクリックします。

ステップ 4 [OK] をクリックしてドメインに強制適用する設定を保存します。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

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。

デバイスにアクセス コントロール ポリシーを割り当てる

アクセス コントロール ポリシーは、それを使用するデバイスを指定します。各デバイスは、1つのアクセス コントロール ポリシーのみに割り当てることができます。デバイステンプレー

トにポリシーを割り当てることもできます。テンプレートは、使用可能な選択済みデバイスのリストに含まれています。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、**[ターゲット：x デバイス（Targeted: x devices）]** リンクをクリックします。

ステップ 2 ターゲット リストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。
- 削除：1 つのデバイスの横にある **Delete** () をクリックするか、複数のデバイスを選択して、右クリックしてから **[選択項目の削除（Delete Selection）]** を選択します。
- 検索：検索フィールドに検索文字列を入力します。検索をクリアするには、**Clear** () をクリックします。

[影響を受けるデバイス（Impacted Devices）] の下に、割り当てられたアクセス コントロール ポリシーが現在のポリシーの子であるデバイスが一覧表示されます。現在のポリシーを変更すると、これらのデバイスに影響します。

ステップ 3 [OK] をクリックしてターゲット デバイス設定を保存します。

ステップ 4 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

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。

アクセス コントロール ポリシーのロギング設定

アクセス コントロール ポリシーのロギング設定を構成するには、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [ロギング（Logging）] を選択します。

アクセス コントロール ポリシーのデフォルトの syslog 宛先と syslog アラートを設定できます。この設定は、syslog の宛先設定が組み込まれているルールとポリシーのカスタム設定で明示的にオーバーライドされない限り、アクセス コントロール ポリシーと組み込まれているすべての復号、プレフィルタ、および侵入ポリシーに適用されます。

デフォルトアクションで処理される接続のロギングは、初期設定では無効です。

IPS とファイルおよびマルウェアの設定は通常、syslog メッセージの送信についてページ上部のオプションを選択した後に有効になります。

デフォルト Syslog 設定

ポリシーにデフォルトのSyslog サーバーを構成するには、**[Syslog サーバー（Syslog Server）]** オプションを選択します。次に、接続先と必要に応じてアラート レベルを選択します。選択できるオプションは、次のとおりです。

- **特定のsyslogアラートを使用して送信**する：このオプションを選択すると、『*Cisco Secure Firewall Management Center Administration Guide*』の「*Creating a Syslog Alert Response*」の手順で設定したとおりに、選択したsyslogアラートに基づいてイベントが送信されます。リストから syslog アラートを選択するか、名前、ロギング ホスト、ポート、機能および重大度を指定することにより syslog アラートを追加できます。詳細については、*Cisco Secure Firewall Management Center Administration Guide*の「*Facilities and Severities for Intrusion Syslog Alerts*」を参照してください。

  このオプションを使用すると、システムは管理インターフェイスを使用して syslog メッセージをサーバーに送信します。管理インターフェイスからsyslogサーバーへのルートがあることを確認します。ルートがあると、メッセージがサーバーに届きません。

- を使用：このオプションを選択して**[重大度（Severity）]**を選択すると、接続または侵入イベントが選択した重大度とともにプラットフォーム設定で設定したsyslogコレクタに送信されます。このオプションを使用し、プラットフォーム設定で行ったsyslog構成を統合して、アクセス コントロール ポリシーでその設定を再利用できます。このセクションで選択した重大度はすべての接続イベントと侵入イベントに適用されます。デフォルトの重大度は ALERT です。

侵入設定

- **Send Syslog messages for intrusion (IPS) イベント**：syslog メッセージとして侵入イベントが送信されます。上記で設定したデフォルトは、オーバーライドしない限り使用されます。

- **[オーバーライドの表示/非表示（Show/Hide Overrides）]**：デフォルトのsyslog宛先と重大度を使用する場合は、これらのオプションを空のままにします。それ以外の場合は、侵入イベントに別のsyslogサーバーの宛先を設定し、イベントのシビラティ（重大度）を変更できます。

ファイルおよびマルウェアの設定

- [ファイルおよびマルウェアイベントのsyslogメッセージを送信（Send Syslog messages for File and Malware events）]：ファイルおよびマルウェアイベントを syslog メッセージとして送信します。上記で設定したデフォルトは、オーバーライドしない限り使用されます。

- **[オーバーライドの表示/非表示（Show/Hide Overrides）]**：デフォルトのsyslog宛先と重大度を使用する場合は、これらのオプションを空のままにします。それ以外の場合は、ファイルおよびマルウェアイベントに別のsyslogサーバーの宛先を設定し、イベントの重大度を変更できます。

アクセス制御への他のポリシーの関連付け

主要ポリシーをアクセス コントロール ポリシーに関連付ける最も簡単な方法は、アクセス コントロール ポリシーのトピックに示されているパケット フローでポリシーのリンクをクリックすることです。関連付けるポリシーをすばやく選択できます。または、このトピックで説明されているように、ポリシーの詳細設定を使用してポリシーを関連付けることもできます。これらのポリシーには以下が含まれます。

- プレフィルタ ポリシー：（レイヤ4の）アウターヘッダによりネットワーク限定を使用した早期のトラフィック処理を実行します。
- 復号ポリシー：セキュアソケットレイヤ（SSL）または Transport Layer Security（TLS）で暗号化されたアプリケーション層プロトコルトラフィックをモニタ、復号、ブロック、または許可します。
- アイデンティティポリシー：トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザー識別を実行します。

始める前に

SSL ポリシーをアクセス コントロール ポリシーに関連付ける前に、TLS サーバーアイデンティティ検出で TLS サーバ アイデンティティ検出に関する情報を確認してください。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 適切な [ポリシー設定（Policy Settings）] 領域の **Edit** (✎) をクリックします。

代わりに **View** (👁) が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 ドロップダウン リストからポリシーを選択します。

ユーザーが作成したポリシーを選択する場合は、表示される編集アイコンをクリックしてポリシーを編集できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

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。

ポリシー アナライザとオプティマイザを使用した異常の特定と修正

ポリシーアナライザとオプティマイザを使用して、冗長ルールやシャドウルールなどの異常に対するアクセス コントロール ポリシーを評価し、検出された異常を修正するアクションを実行できます。ポリシーアナライザとオプティマイザはクラウドでホストされており、クラウドと統合されていない場合に使用できるルール分析とは異なります。クラウドと統合すると、非クラウドのポリシー分析は使用できなくなります。

ポリシー分析は毎日（24時間ごとに）自動で実行されます。分析を手動で開始することもできます。最初にサービスを有効にしたときは、既存のすべてのアクセス コントロール ポリシーの分析が開始されます。

（注） ポリシーを最適化する前には、ポリシーのコピーを作成します。最適化の結果に満足できない場合、管理対象デバイスをそのコピーに再割り当てし、簡単にシステムを開始状態に戻すことができます。

始める前に

- Firewall Management Center 7.2 以降では、Security Cloud Control から直接ポリシーアナライザとオプティマイザを使用できますが、この機能を相互起動できるのは7.6以降のみです。アクセス コントロール ポリシーに割り当てられた管理対象デバイスで実行されているソフトウェアバージョンは関係ありません。ポリシーアナライザとオプティマイザはクラウドのみでホストされるため、Firewall Management Center 内から分析を実行しても、Security Cloud Control から直接実行しても違いはありません。
- この機能を使用するには、Cisco Security Cloud と統合するときに、**Integration** > **Cisco Security Cloud** で **[ポリシー分析と最適化を有効にする（Enable Policy Analysis & Optimization）]** を選択する必要があります。
- 変更管理を有効にしている場合、ポリシーアナライザとオプティマイザは変更のチケットを自動的に作成し、チケットを送信します。変更を展開する前に、承認者がチケットを承認する必要があります。
- ドメインを使用している場合、[異常（Anomaly）] 列のリンクをクリックしてレポートを表示することはできません。代わりに、Security Cloud Control にログインし、そのアプリケーションの機能を使用します。
- ポリシーアナライザとオプティマイザは、更新、無効化、またはマージされたルールにルールコメントを追加します。後でこれらのコメントを検索して、最適化されたルールを見つけることができます。
- ポリシーアナライザとオプティマイザによって導入された変更は、デフォルト名 internaladmin で API コールとして監査ログに反映されます。

手順

ステップ 1 **Policies** > **Access Control heading** > **Access Control**を選択します。

すでに分析を実行している場合、[異常（Anomaly）] 列には、ポリシーの問題の数、ポリシーを最適化できる割合、およびポリシー分析の状態（[エラー（Error）] や [完了（Completed）] など）が表示されます。[最終分析日（Last Analyzed）] には、分析が実行された日時が表示されます。

ステップ 2 1 つ以上のポリシーを選択し、[ポリシーの分析（Analyze Policy）] をクリックします。

分析は、クラウドのバックグラウンドプロセスとして実行されます。分析が完了すると、[異常（Anomaly）] 列に結果が表示されます。

注：

- **[分析（Analyze）] > [ポリシー（Policy）]** を選択して、ポリシーの編集時に分析を開始することもできます。そのメニューの他のオプションを使用すると、ヒットカウントと警告を表示できます。
- クラウドにまだ接続していない場合は、このボタンをクリックすると開く説明ダイアログに [統合（Integrate）] ボタンが含まれており、開始することができます。ポリシーアナライザとオプティマイザはクラウドでのみ動作します。

ステップ 3 分析が完了したら、[異常（Anomaly）] 列の [%最適化可能（% Optimizable）] リンクをクリックして、クラウドでポリシーアナライザとオプティマイザを起動します。

実行するすべてのアクションを完了したら、（クラウドで）[修復を適用（Apply Remediations）] をクリックします。実行内容の確認が表示されます。[続行（Proceed）] をクリックして変更を実装します。

最初の分析がエラーで終了した場合は、代わりに [再分析（Re-analyze）] をクリックしてプロセスを再開できます。

ステップ 4 ポリシーを展開して変更を完了します。

変更管理が有効になっている場合、承認者は、修復を展開する前に、まず修復を含むチケットを承認する必要があります。

ルール ヒット カウントの表示

ヒットカウントは、ポリシールールまたはデフォルトアクションが接続に一致した回数を示します。ヒットカウントは、ルールに一致する接続の最初のパケットに対してのみ増加します。この情報を使用してルールの有効性を特定することができます。ヒットカウント情報は、Firewall Threat Defense デバイスに適用されるアクセス制御とプレフィルタルールに対してのみ使用できます。

（注）
- このカウントは、再起動やアップグレードの後も維持されます。
- カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。
- デバイスで展開またはタスクが進行中の場合、デバイスからヒットカウント情報を取得することはできません。
- また、デバイス CLI で **show rule hits** コマンドを使用してルールヒットカウント情報を表示することもできます。
- [アクセスコントロールポリシー（Access Control Policy）] ページから [ヒットカウント（Hit Count）] ページにアクセスした場合、プレフィルタ ルールを表示または編集することはできません。また、その逆も同様です。
- ヒットカウントは、モニターアクションを使用するルールでは使用できません。

始める前に

カスタムユーザーロールを使用する場合は、ロールに次の権限が含まれていることを確認してください。

- デバイスの閲覧：ヒットカウントを確認します。
- デバイスの変更：ヒットカウントを更新します。

手順

ステップ 1 アクセス制御ポリシーまたはプレフィルタ ポリシー エディタで、ページの右上にある **[ルールヒット数の > 分析（Analyze）]]**をクリックします。

ステップ 2 [ヒット カウント（Hit Count）] ページで、[デバイスの選択（Select a device）] ドロップダウンリストからデバイスを選択します。

このデバイスのヒットカウントを生成するのが初めてではない場合は、ドロップダウンボックスの横に最後に取得したヒットカウント情報が表示されます。また、[最終展開（Last Deployed）] の時刻を確認して、最新のポリシー変更を確認します。

ステップ 3 必要に応じて、**Refresh**（ ）をクリックして、選択したデバイスから現在のヒットカウントデータを取得します。

プレフィルタポリシーでは、[現在のヒットカウントの取得（Fetch Current Hit Count）] をクリックして、最初のヒットカウントデータを取得する必要がある場合があります。

デバイスへの展開が進行している間は、ヒットカウントを更新できません。

ステップ 4 データを表示して分析します。

次を実行できます。

- [プレフィルタ（Prefilter）] または **[アクセス制御（Access Control）]** をクリックして、これらのポリシーのヒットカウントを切り替えます。
- [フィルタ（Filter）] ボックスに検索文字列を入力して、特定のルールを検索します。
- [フィルタ基準（Filter by）] フィールドで [ヒットルール（Hit Rules）] や [ルールにヒットしない（Never Hit Rules）] オプションを選択して、リストを大まかに制限します。ヒットルールを閲覧するときに、[最後（In Last）] フィールドで時間範囲を選択することで（たとえば、過去 1 日）、リストをさらに制限できます。
- （アクセスコントロールポリシーから見た場合）ルールのチェックボックスをオンにし、[ヒットカウントのクリア（Clear Hit Counts）] をクリックして、1 つ以上のルールのヒットカウントをクリアします。アクションを確認したら、[クリアしてリロードする（Clear and Reload）] を選択してヒットカウントデータを更新します。一度に最大 500 のルールのヒットカウントをクリアできます。ヒットカウントのクリアを元に戻すことはできません。

  （注）
  テーブルヘッダーのチェックボックスをクリックしてリスト内のすべてのルールを選択します。ルールの範囲を選択するには、最初のルールのチェックボックスを選択し、Shift キーを押しながら最後のルールのチェックボックスをクリックします。間にあるすべてのルールも選択されます。

- （アクセスコントロールポリシーから見た場合）個々のルールで次の操作を実行できます。
  - **More** (⋮) メニューから [編集（Edit）] をクリックして、ルールを編集します。
  - **More** (⋮) メニューから [削除（Delete）] をクリックして、ポリシーからルールを削除します。
  - **More** (⋮) メニューから [ルールの有効化/無効化（Enable/Disable Rule）] をクリックして、ルールを有効化または無効化します。
  - **More** (⋮) メニューから [ヒットカウントのクリア（Clear Hit Count）] をクリックして、ヒットカウントをクリア（ゼロにリセット）します。この操作は取り消すことができません。
- （プレフィルタポリシーから見た場合）**Cog** (⚙) をクリックして表示する列を選択することで、表示される列を変更します。
- （プレフィルタポリシーから見た場合）ルール名をクリックして編集するか、最後の列の **View** (👁) をクリックしてルールの詳細を表示します。ルール名をクリックすると、ポリシー ページ内でその名前がハイライトされ、編集できるようになります。
- （プレフィルタポリシーから見た場合）ルールを右クリックし、[ヒットカウントのクリア（Clear Hit Count）] を選択してルールのヒットカウント情報をクリア（ゼロにリセット）します。Ctrl を押しながらクリックすることで、複数のルールを選択できます。この操作は取り消すことができません。

- ページの左下にある [CSVの生成（Generate CSV）] をクリックして、詳細情報のカンマ区切り値のレポートをページ上で生成します。

ステップ 5 [閉じる（Close）] をクリックしてポリシー ページに戻ります。

ルールの競合および警告の分析

（注） このトピックで説明する機能は、Cisco Security Clound を統合していない場合にのみ使用できます。クラウドと統合すると、この機能はより強力なポリシーアナライザおよびオプティマイザに置き換えられます。ポリシー アナライザとオプティマイザを使用した異常の特定と修正（23 ページ）を参照してください。

ルール競合に関する警告および情報を表示して、アクセス コントロール ポリシーのロジックを調べ、変更が必要なルールを特定することができます。ルールが重複していると、不要なルールがポリシーに含まれることになる場合があり、それらのルールがトラフィックに一致することはありません。分析は、不要なルールを削除したり、目的のポリシーを適用するために移動または変更する必要があるルールを特定するために役立ちます。

ポリシーの警告とエラーは、ルールが目的のサービスを確実に提供するために理解し、多くの場合に対処する必要がある事柄を示します。

ルール競合分析では、次のタイプの問題が特定されます。

- オブジェクトの重複：ルールのフィールドに含まれる 1 つの要素が、ルールの同じフィールドに含まれる 1 つ以上の要素のサブセットになっています。たとえば、送信元フィールドには、10.1.1.0/24 のネットワークオブジェクトと、ホスト 10.1.1.1 の別のオブジェクトが含まれる場合があります。10.1.1.1 は 10.1.1.0/24 によってカバーされるネットワーク内にあるため、10.1.1.1 のオブジェクトは冗長であり、削除することができます。それにより、ルールが簡素化され、デバイスのメモリも節約できます。
- 冗長なルール：基本ルールでも 2 つのルールによって同じタイプのトラフィックに同じ処理が適用される場合、基本ルールを削除しても最終的な結果は変わりません。たとえば、特定のネットワークの FTP トラフィックを許可するルールに、同じネットワークの IP トラフィックを許可するルールが続き、その間にアクセスを拒否するルールがない場合、最初のルールは冗長であり、削除できます。
- シャドウイング状態のルール：これは、冗長なルールの逆です。この場合は、あるルールが別のルールと同じトラフィックに一致し、2 番目のルールはアクセス リスト内であとに配置されているためにいずれのトラフィックにも適用されません。両方のルールのアクションが同じである場合は、シャドウイング状態のルールを削除できます。2 つのルールがトラフィックに対して異なるアクションを指定している場合、必要なポリシーを導入するには、シャドウイング状態のルールを移動するか、いずれかのルールの編集が必要になる場合があります。たとえば、1 つの送信元または宛先に対して、基本ルールで IP トラ

フィックを拒否し、シャドウイング状態のルールでFTPトラフィックを許可する場合などです。

始める前に

分析を実行する場合：

- ルールごとに最初の競合のみが識別されます。問題を修正すると、そのルールがテーブル内の別のルールと競合していると識別される場合があります。ただし、1 つのルールに複数の警告またはエラーがある場合があります。
- ルール競合分析では、送信元/宛先のセキュリティゾーン、ネットワーク、VLAN、およびサービス/ポートの一致条件とアクションのみが考慮されます。他の一致基準は考慮されないため、一見冗長なルールが完全に冗長ではない可能性があります。
- FQDN の IP アドレスは DNS ルックアップの前に知ることができないため、FQDN ネットワークオブジェクトの競合は分析できません。
- 無効になっているルールは無視されます。
- 時間範囲属性は無視されます。異なる期間のルールは、実際にはその時間範囲で冗長ではない場合でも、冗長としてマークされる可能性があります。
- 警告およびエラーとルール競合（機能を有効にする場合）のアイコンがルールテーブルに表示されます。アイコンのリファレンスについては、ルールおよび他のポリシー警告 （6 ページ）を参照してください。

手順

ステップ 1 **Policies** > **Access Control heading** > **Access Control** を選択し、アクセス コントロール ポリシーを編集します。

ステップ 2 次のいずれかを実行して、ルールの競合および警告のダイアログボックスを開きます。

- ルール競合を表示するには、[分析（Analyze）] ドロップダウンをクリックし、[ルールの競合を有効にする（Enable Rule Conflicts）] をクリックします。分析が完了すると、ページの上部に競合の概要が表示されます。次に、同じメニューから [ルールの競合の表示（Show Rule Conflicts）] をクリックして、特定の結果を表示します。

  ポリシーを開くたびに、またはポリシーに変更を加えて保存するたびに、ルール競合の検出を再度有効にする必要があります。

- ルールの警告およびエラーを表示するには、**[分析（Analyze）]** > **[警告とエラーの表示（Show Warnings and Errors）]** をクリックします。

  ポリシーに変更を加えた後、[分析（Analyze）] ボタンの横にあるリロードアイコンをクリックして結果を更新できます。

- ポリシーの警告を表示するには、**[分析（Analyze）]**>**[ポリシーの警告の表示（Show Policy Warnings）]** をクリックします。
- ルール競合の確認が完了したら、**[分析（Analyze）]**>**[ルールの競合を無効にする（Disable Rule Conflicts）]** をクリックします。

ステップ 3 ルールの競合および警告のダイアログボックスには、次のような機能があります。

- ルールの警告とエラーは、ルールの競合とは別のタブに表示されます。ポリシー警告用の別のタブもあります。
- 各タブにはサブタブがあり、問題の個別のタイプ（冗長かシャドウイングか、警告かエラーか、など）を調べることができます。アイテムを検索することもできます。
- 各ルール名の横にある **More** (⋮) は、ルールの編集、無効化、または削除へのショートカットを提供します。

ステップ 4 終了したら、[閉じる（Close）] をクリックします。

ルールの検索

検索を使用してルールを見つけることができ、ルールの数が多い場合は特に役立ちます。

送信元または宛先ネットワークで IP アドレスを（簡易テキスト検索ではなく）検索すると、アドレスに一致するルールが返されます。対象には、完全一致だけでなく、サブネット一致も含まれます。たとえば、10.1.1.1 を検索すると、10.1.1.0/24 のルールも結果に含まれます。

手順

ステップ 1 アクセスコントロールポリシーを編集するときは、[検索（Search）]ボックスをクリックして検索文字列を作成します。

- 単純なテキスト文字列検索の場合は、文字列を入力します。検索では、検索文字列がいずれかの列にあるルールが返されます。文字列検索と送信元ネットワーク検索を組み合わせるなど、文字列検索とタグ検索は同時に使用できません。
- 特定の列を検索するには、完全な名前（送信元ネットワークなど）の入力を求められるまで列名を入力するか、検索可能なフィールドのリストから名前を選択します。検索タグを選択すると、そのタグの検索文字列を入力できます。例：**送信元ネットワーク 10.1.1.1**。
- ポート フィールドで検索すると、完全一致のみが返されます。
- 複数の値を入力する場合は、値をカンマで区切ります。
- 最初の検索後、検索ボックスをクリックすると、最近の検索とタグが表示されます。検索を選択してすばやく繰り返したり、以前の検索やタグを選択してそれらに基づいて同様の検索を作成したりできます。

- 複数のタグで検索文字列を作成する場合は、タグの間にスペースを含めないでください。
- タグを選択すると、対象の列に表示される値を求めるプロンプトが表示されます。検索する値を選択します。
- 検索ボックスの左側にある [フィルタ（FIlter）] アイコンをクリックし、[許可（Allow）]、[ブロック（Block）]、[モニター（Monitor）]、[侵入ポリシー（Intrusion Policy）]、[時間範囲（Time Range）]、[競合（Conflicts）]、[警告（Warnings）]、[エラー（Errors）]、[無効（Disabled）] ルール、期限切れのルール、定義が重複しているオブジェクトを含むルールの任意の組み合わせでルールを表示するように選択することにより、一部の一般的な機能に基づいてすばやくフィルタ処理できます。.
- 特定のデバイスまたは一連のデバイスに適用されるルールを表示するには、[フィルタ（FIlter）] アイコンをクリックしてデバイスを選択します。デバイス上に少なくとも 1 つのインターフェイスを含むセキュリティゾーンを使用している場合、またはセキュリティゾーンが含まれていない場合、ルールはそのデバイスに適用されます。

ステップ 2 検索ボックスの検索文字列の末尾にカーソルを置き、Enter を押します。

検索文字列に一致するルールは強調表示され、一致しないルールは非表示になります。[一致するルールのみを表示（Show Only Matching Rules）] の選択を解除すると、テーブル全体が表示され、テーブル内のルールが強調表示され、周囲のルールを確認できます。

[一致するルールのみを表示（Show Only Matching Rules）] チェックボックスの横には、ポリシー内のルールの総数と検索文字列に一致する数の比較に関する概要が表示されます。

ステップ 3 検索を閉じて、フィルタ処理も強調表示もされていないテーブルに戻るには、検索ボックスの右側にある [X] をクリックします。検索文字列の末尾にカーソルを置き、Esc キーを押すこともできます。

アクセス コントロール ポリシーの履歴

表 3:

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Object group search performance enhancements.	7.6.0	7.6.0	Object group search is now faster and uses fewer CPU resources. New CLI commands: **clear asp table network-object**, **show asp table network-object**, **debug acl ogs** Modified CLI comments (enhanced output): , **packet-tracer**, **show access-list**, **show object-group**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Policy Analyzer & Optimizer for access control.	Management Center 7.6.0 以降 Security Cloud Control 7.2.0 以降	任意（Any）	The Policy Analyzer & Optimizer evaluates access control policies for anomalies such as redundant or shadowed rules, and can take action to fix discovered anomalies. You can launch the access control Policy Analyzer & Optimizer directly from a Version 7.6+ Firewall Management Center; this requires Cisco Security Cloud. For Versions 7.2–7.4 Firewall Management Centers, use Security Cloud Control. New/modified screens: • To enable: **Integration** > **Cisco Security Cloud** > **Enable Policy Analyzer & Optimizer** • To analyze policies: **Policies** > **Access Control**, select policies, click **Analyze Policies**.
アクセスコントロールポリシーとルールを変更するための詳細なアクセス許可。	7.4.0	任意（Any）	カスタムユーザーロールを定義して、アクセスコントロールポリシーおよびルールの侵入設定と、その他のアクセスコントロールポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。 ユーザーロールを定義するときに、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセスコントロールポリシー（Access Control Policy）]** > **[アクセスコントロールポリシーの変更（Modify Access Control Policy）]** > **[脅威設定の変更（Modify Threat Configuration）]**オプションを選択して、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、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 ポリシーの構成、およびポリシーのデフォルトアクションの侵入アクションを選択できるようにします。[残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] を使用して、ポリシーの他のすべての側面を編集する機能を制御できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、引き続きすべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。
新しいアクセスコントロールポリシーのユーザーインターフェイスとルールの競合分析。	7.3.0	いずれか	7.2 で導入されたアクセス コントロール ポリシーのユーザーインターフェイスは、デフォルトのインターフェイスになりました。また、ルールの競合分析を有効にすると、ポリシーでの以前ルールが原因で一致しない冗長ルールやオブジェクト、およびシャドウルールを特定できます。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
アクセスコントロールポリシーのロック。	7.2.0	いずれか	アクセス コントロール ポリシーをロックして、他の管理者が編集できないようにすることができます。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。アクセス コントロール ポリシーを変更する権限を持つすべてのユーザーには、それをロックする権限があります。 ポリシーの編集時にポリシーをロックまたはロック解除するアイコンがポリシー名の横に追加されました。さらに、他の管理者によってロックされたポリシーのロックを解除できるようにする新しい権限（アクセス コントロール ポリシー ロックのオーバーライド）が追加されました。この権限は、デフォルトで管理者、アクセス管理者、およびネットワーク管理者のロールで有効になっています。
ルールのヒットカウントは再起動後も存続します。	7.2.0	いずれか	管理対象デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。**show rule hits** コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。 次のデバイス CLI コマンドを変更しました：**show rule hits**。
アクセスコントロールポリシーのユーザビリティの改善。	7.2.0	いずれか	アクセスコントロールポリシーで使用できる新しいユーザーインターフェイスが追加されました。従来のユーザーインターフェイスを引き続き使用することも、新しいユーザーインターフェイスを試すこともできます。新しいインターフェイスは、ルールリストのテーブルビューとグリッドビュー、列を表示または非表示にする機能、高度な検索機能、無限スクロール機能を備え、アクセス コントロール ポリシーが割り当てられたポリシーに関するパケットフローのビューがより明確になりました。また、ルール作成用の追加/編集ダイアログボックスがシンプルになりました。アクセスコントロールポリシーの編集中に、従来のユーザーインターフェイスと新しいユーザーインターフェイスを自由に切り替えることができます。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
DNS フィルタリング	7.0.0 6.7.0（試験的）	任意（Any）	URL フィルタリングが有効になっていて設定されている場合、カテゴリとレピュテーションのフィルタリングの有効性を強化する新しいオプションが、新しい各アクセス コントロール ポリシーでデフォルトで有効になっています。 詳細については、DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別とサブトピックを参照してください。 [全般設定（General Settings）] の下のアクセス コントロール ポリシーの [詳細（Advanced）] タブに、[DNSトラフィックへのレピュテーション適用を有効にする（Enable reputation enforcement on DNS traffic）] という新しいオプションが追加されました。
TLS サーバーアイデンティティ検出	6.7.0	いずれか	クライアントが TLS 1.3 対応サーバーに接続するときに、アクセス コントロール ポリシーを有効にして URL とアプリケーションの条件を評価します。TLS サーバーアイデンティティ検出により、トラフィックを復号せずにこれらの条件を評価できます。 この機能を有効にすると、モデルによっては、デバイスのパフォーマンスに影響する可能性があります。 アクセス コントロール ポリシーの [詳細設定（Advanced）] タブページに、新しいオプションが追加されました。 • [詳細設定（Advanced）] タブに警告が表示されます。スライダを右に動かすと、TLS サーバーアイデンティティ検出が有効になります。 • [詳細設定（Advanced）] タブページに、[TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）] という新しいオプションが追加されました。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
新しいセキュリティインテリジェンスカテゴリ	—	任意	次のカテゴリは6.6リリースの頃に導入されましたが、6.6に限定されてはいません。 • banking_fraud • high_risk • ioc • link_sharing • malicious • newly_seen • spyware

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。