アクセス制御ポリシー

ここでは、アクセス コントロール ポリシーを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（Name）と説明（Description）

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（Inheritance Settings）

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。

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（Default Action）

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（HTTP Responses）

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 の宛先設定で組み込まれているルールおよび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 SSL、プレフィルタ、および侵入のポリシーに適用されます。

アクセス コントロールの詳細オプション（Advanced Access Control Options）

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、SSL インスペクション、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。

システム作成のアクセス コントロール ポリシー

デバイスの初期設定に応じて、システム付属のポリシーには次のものが含まれます。

- デフォルトアクセス制御：詳細な検査なしで、すべてのトラフィックをブロックします。

- デフォルト侵入防御：すべてのトラフィックを許可しますが、Balanced Security and Connectivity 侵入ポリシーおよびデフォルトの侵入変数セットを使用して検査も実行します。
- デフォルトネットワーク検出：すべてのトラフィックを許可すると同時に検出データについて検査しますが、侵入やエクスプロイトについては検査しません。

アクセス コントロール ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

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 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（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。

- 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 （4 ページ）を参照してください。
- 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：[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（5 ページ）を参照してください
- 削除：[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。
- [コピー（Copy）]：[その他（More）] メニューから [複製（Clone）] を選択します。[コピー（Copy）]（） をクリックします。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）]：[その他（More）] メニューから [レポートの生成（Generate Report）] を選択します。**[レポート（Report）]**（） 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 （8 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 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

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 オプションで、[基本ポリシーの選択（Select Base Policy）] ドロップダウンリストから基本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 必要に応じて、ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリック（またはドラッグ アンド ドロップ）して、選択したデバイスを追加します。表示されるデバイスを絞り込むには、[検索（Search）] フィールドに検索文字列を入力します。

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 （5 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。

（注） ポリシーをロックしない場合は、次の点を考慮してください。ポリシーの編集は、1 つのブラウザウィンドウを使用して、一度に1人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。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。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（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 [編集（Edit）]（✎） をクリックします。

代わりに [表示（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 [アクションの選択（Select Action）] 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、クローン作成、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。

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 [編集（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 アクション：[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ます。
- デフォルトアクションの設定：[歯車（Cog）]（⚙） をクリックして変更を加え、[OK] をクリックします。ロギング、外部 syslog サーバーまたは SNMP トラップサーバーの場所、および侵入防御のデフォルトアクションに関連付けられた変数セットの設定を行えます。
- 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：xデバイス（Targeted: x devices）] リンクをクリックします。
- 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 [その他（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削除するには、[空の列を非表示（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。
- ルールのロジックを分析します。[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。
  - [ヒットカウント（Hit Count）]：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。
  - [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。
  - [警告を表示（Show Warnings）]：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。
- 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、SSLインスペクション、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 （15 ページ）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 （10 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（11 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。

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、次の権限によって制御される必要があります。**[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）]>[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（Override Access Control Policy Lock）]**。

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

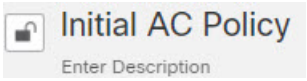
ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]**を選択します。

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 [編集（Edit）]（✎）をクリックします。

[ロックステータス（Lock Status）]列には、ポリシーがすでにロックされているかどうか、ロックされている場合は誰がロックしたかが表示されます。空のセルは、ポリシーがロックされていないことを示します。

代わりに [表示（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。
- [階層内のこのポリシーと親のロック/ロック解除（Lock/Unlock This Policy and Parents in the 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 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 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 （5 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 （10 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 （11 ページ） で説明する手順を実行します。
- ドメインで必須：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個のデバイス（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 （12 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、[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ドロップダウン矢印から [HTTP応答（HTTP Responses）] または [詳細設定（Advanced Settings）] を選択し、基本ポリシーからアクセス コントロール ポリシー設定を継承する （11 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。

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。

基本ポリシーからアクセス コントロール ポリシー設定を継承する

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）] 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。

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。

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 ポリシーのエディタで、[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 [削除（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、[クリア（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。

アクセス コントロール ポリシーのターゲット デバイスの設定

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。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。

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、[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 [ターゲットデバイス（Targeted Devices）] で、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 [削除（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 [選択済み項目の削除（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、[クリア（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 SSL/TLS 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

- [特定のsyslogアラートを使用して送信する（Send using specific syslog alert）]：このオプションを選択すると、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』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 アドミニストレーション ガイドの「*Facilities and Severities for Intrusion Syslog Alerts*」を参照してください。このオプションはすべてのデバイスに適用されます。

  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。

- [デバイスに展開したFTDプラットフォーム設定のポリシーで指定されているsyslog設定を使用（Use the syslog settings configured in the FTD Platform Settings policy deployed on the device）]：このオプションを選択してシビラティ（重大度）を選択すると、接続または侵入イベントが選択したシビラティ（重大度）とともに [プラットフォーム設定（Platform Settings）] 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（Platform Settings）] で行った syslog 設定を統合して、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。

  このオプションは、Secure Firewall Threat Defense デバイス 6.3 以降のみに適用されます。

IPS 設定

- [IPSイベントのsyslogメッセージを送信（Send Syslog messages for IPS events）]：IPS 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、IPS 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。

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 コントロール ポリシーの詳細設定

アクセス コントロール ポリシーの詳細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 [詳細設定（Advanced Settings）] を選択します。

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。デフォルト設定は、ほとんどの展開環境に適しています。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Update Intrusion Rules*」で説明しているように、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オプションの多くは、ルールの更新によって変更される可能性があることに注意してください。

代わりに[表示（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。

⚠

注意 Snort プロセスを再起動し、トラフィック インスペクションを一時的に中断する詳細設定変更のリストについては、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 を参照してください。 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を参照してください。

親ポリシーからの設定の継承

アクセス コントロール ポリシーにベースポリシーがある場合は、ベースポリシーから設定を継承することができます。親ポリシーの設定を使用する設定グループごとに、[ベースポリシーから継承（Inherit from base policy）] を選択します。これらの設定がロックされるように継承が設定されている場合、これらの設定は読み取り専用になり、ポリシーに固有の設定を行うことはできません。

ポリシーに固有の設定を行うことが許可されている場合、編集するには [ベースポリシーから継承（Inherit from base policy）] を選択解除する必要があります。

全般設定

オプション	説明
接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）	ユーザーが要求した各URLに対して保存する文字数をカスタマイズするには詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Limiting Logging of Long URLs」を参照してください。 ユーザーが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔をカスタマイズするには、ブロックされた Web サイトのユーザー バイパス タイムアウトの設定を参照してください。
インタラクティブブロックを一時的に許可する時間(秒)（Allow an Interactive Block to bypass blocking for (seconds)）	ブロックされた Web サイトのユーザー バイパス タイムアウトの設定 を参照してください。
URL キャッシュのミス検索の再試行（Retry URL cache miss lookup）	システムは、ローカルに保存されたカテゴリとレピュテーションを持たない URL を初めて検出すると、今後その URL をすばやく処理できるように、そのURLをクラウドで検索して結果をローカルデータストアに追加します。 この設定により、クラウドで URL のカテゴリとレピュテーションを検索する必要がある場合の処理が決まります。 デフォルトでは、この設定は有効になっています。システムは、クラウドのURLのレピュテーションとカテゴリをチェックしている間、トラフィックを一時的に遅延させ、クラウドの判定を使用してトラフィックを処理します。 この設定を無効にした場合、ローカルキャッシュに存在しないURLがシステムで検出されると、トラフィックはただちに渡され、未分類およびレピュテーションのないトラフィック用に設定されたルールに従って処理されます。 パッシブ展開では、システムはルックアップを再試行しません。これは、システムがパケットを保持できないからです。
Threat Intelligence Director を有効にする（Enable Threat Intelligence Director）	このオプションを無効にすると、設定したデバイスへの TID データの公開が停止されます。
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）	このオプションは、URL フィルタリングのパフォーマンスと有効性を向上させるために、デフォルトで有効になっています。詳細および追加手順については、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（ベータ版）およびサブトピックを参照してください。

オプション	説明
ポリシー適用中のトラフィックの検査	特定の設定でSnortプロセスを再起動する必要がない限り設定の変更を展開する場合にトラフィックを検査するには、必ず、[ポリシーの適用時にトラフィックを検査する（Inspect traffic during policy apply）] がデフォルト値（有効）に設定してください。 このオプションを有効にすると、リソースの需要が高まった場合にいくつかのパケットが検査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。詳細については、Snort再起動のシナリオを参照してください。

関連するポリシー

詳細設定を使用して、サブポリシー（復号、アイデンティティ、プレフィルタ）をアクセス制御に関連付けます。「アクセス制御への他のポリシーの関連付け （21 ページ）」を参照してください。

TLS サーバーアイデンティティ検出

RFC 8446 で定義されている最新バージョンの Transport Layer Security（TLS）プロトコル 1.3 は、セキュアな通信を提供するために多くのWebサーバーで採用されているプロトコルです。TLS 1.3プロトコルが、セキュリティを強化するためにサーバーの証明書を暗号化する一方で、証明書が、アクセスコントロールルールのアプリケーションおよびURL フィルタリング基準に適合する必要があるため、Firepower システムは、パケット全体を復号せずにサーバー証明書を抽出する方法を提供します。

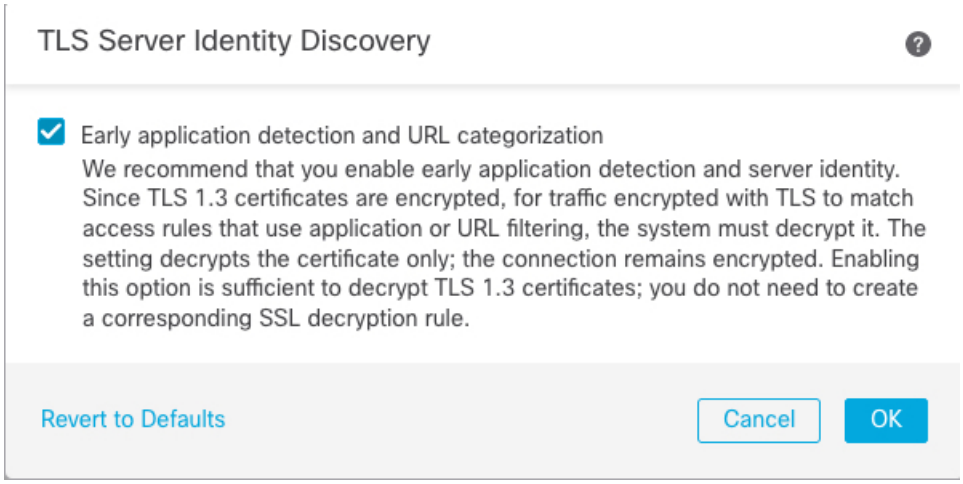
アクセス コントロール ポリシーの詳細設定を指定する場合に、この「TLS サーバーアイデンティティ検出」と呼ばれる機能を有効にできます。

このオプションを有効にする場合は、復号ポリシーの高度な TLS 適応型サーバーのアイデンティティ プローブ オプションも有効にすることをお勧めします。これらのオプションを組み合わせることで、TLS 1.3 トラフィックのより効率的な復号が可能になります。詳細については、TLS 1.3 復号のベストプラクティスを参照してください。

TLSサーバーアイデンティティ検出の影響を受ける新しい接続が開始されると、Firewall Threat Defense は元の ClientHello パケットを保持して、接続先のサーバーのアイデンティティを判別してから続行します。Firewall Threat Defense デバイスは、Firewall Threat Defense からサーバーに特殊な接続を送信します。サーバーの応答にはサーバー証明書が含まれ、特殊な接続が終了し、アクセス コントロール ポリシーの要求に応じて元の接続が評価されます。

TLS サーバー ID 検出では、 サーバー名表示（SNI）よりも証明書の共通名（CN）が優先されます。

TLS サーバーアイデンティティ検出を有効にするには、[詳細（Advanced）] タブをクリックし、設定の[編集（Edit）]（✎）をクリックして[早期アプリケーション検出とURL分類（Early application detection and URL categorization）] を選択します。



この機能は、アプリケーションまたは URL の基準に適合させたいトラフィックに関して、特にそのトラフィックの詳細な検査を実行する必要がある場合に、有効にすることを強くお勧めします。サーバー証明書を抽出するプロセスでトラフィックが復号されないため、復号ポリシー は必要ありません。

（注）

- 証明書は復号されているため、ハードウェアプラットフォームによっては、TLSサーバーアイデンティティ検出によってパフォーマンスが低下する場合があります。
- TLSサーバーアイデンティティ検出は、インラインタップモードまたはパッシブモードの展開ではサポートされません。
- TLS サーバーアイデンティティ検出の有効化は、AWS に展開された Secure Firewall Threat Defense Virtual ではサポートされていません。Secure Firewall Management Center で管理されているそのような管理対象デバイスがある場合、接続イベント **PROBE_FLOW_DROP_BYPASS_PROXY** は、デバイスがサーバー証明書の抽出を試みるたびに増加します。
- TLS サーバーアイデンティティ検出は、TLS 1.2 セッションでも動作します。

ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーおよび侵入ポリシーの詳細設定によって、以下が可能になります。

- パケットを検査するために使用され、システムがトラフィックの検査方法を正確に決定する前に合格する必要がある、侵入ポリシーおよび関連付けられる変数セットの指定。

- 多くの前処理オプションを制御する、アクセス コントロール ポリシーのデフォルト ネットワーク分析ポリシーの変更。
- カスタム ネットワーク分析ルールおよびネットワーク分析ポリシーを使用した、特定のセキュリティ ゾーン、ネットワーク、および VLAN に対する前処理オプションの調整。

詳細については、ネットワーク分析ポリシーと侵入ポリシーに対するアクセス コントロールの詳細設定を参照してください。

Threat Defense サービス ポリシー

Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。このポリシーは Firewall Threat Defense デバイスのみに適用され、その他のデバイス タイプの場合には無視されます。このサービス ポリシー ルールは、アクセス制御ルールの後に適用されます。詳細については、サービスポリシーを参照してください。

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のインスペクション パフォーマンスおよびストレージの調整 に、ファイル制御と マルウェア防御 のパフォーマンス オプションに関する情報が記載されています。

ポートスキャン脅威検出

ポートスキャンディテクタは、あらゆるタイプのトラフィックでポートスキャン アクティビティを検出および防止し、最終的な攻撃からネットワークを保護するために設計された脅威検出メカニズムです。ポートスキャントラフィックは、許可されたトラフィックと拒否されたトラフィックの両方で効率的に検出できます。詳細については、を参照してください。脅威の検出

エレファントフローの設定

エレファントフローは、Snort コアの拘束の原因となる可能性がある、大きくて長期間にわたる高速のフローです。システムストレス、CPU ホグ、パケットドロップなどを軽減するためにエレファントフローに適用できるアクションは 2 つあります。それらのアクションは次のとおりです。

- 一部またはすべてのアプリケーションをバイパスする：このアクションでは、Snort インスペクションからのフローをバイパスします。
- スロットル：このアクションでは、エレファントフローに動的レート制限ポリシー（10% 削減）を適用します。

インテリジェント アプリケーション バイパスの設定

インテリジェント アプリケーション バイパス（IAB）は、トラフィックがインスペクション パフォーマンスとフローしきい値の組み合わせを超過したときにバイパスするアプリケーションを指定する、または、バイパスに関するテストを行うための、エキスパート レベルの設定です。詳細については、インテリジェント アプリケーション バイパスを参照してください。

トランスポート層とネットワーク層のプリプロセッサの設定

トランスポート層とネットワーク層のプリプロセッサの詳細設定は、アクセス コントロール ポリシーが展開されるすべてのネットワーク、ゾーン、VLANにグローバルに適用されます。

- **[接続を追跡する際にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）]**：同じ接続で異なる方向に流れるトラフィックのVLANタグが異なると、トラフィックのリアセンブルやルールの処理に影響を与える場合があります。たとえば、同じ接続のトラフィックをVLAN Aで送信し、VLAN Bで受信することができます。このオプションを選択すると、VLANヘッダーを無視するようにシステムが構成されます。これにより、デプロイメントでパケットを正しく処理できます。

- **[アクティブ応答の最大数（Maximum Active Responses）]**：アクティブ応答を提供するように設定されたプリプロセッサ/侵入ルールをトリガーするTCP接続の場合の、TCP接続ごとのアクティブ応答の最大数。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから[最小応答秒数（Minimum Response Seconds）]を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0に設定すると、追加のアクティブ応答をトリガーするアクティブ応答ルールが無効になります。

- **[応答最小秒（Minimum Response Seconds）]**：**[最大アクティブ応答数（Maximum Active Responses）]**に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を指定します

- **[セッション終了のロギングしきい値（Session Termination Logging Threshold）]**：シスコテクニカルサポートからの指示がない限りこのオプションを変更しないでください。このオプションは、ログに記録されるメッセージのバイト数を指定します。セッションが終了し、メッセージが指定のバイト数を超えた場合は、ログに記録されます。オプションを変更するとシステムパフォーマンスに影響する場合があります。

検出拡張の設定

検出拡張設定は、アダプティブプロファイルをアプリケーション検出とアクセス コントロール ポリシーの侵入ルールに使用するかどうかを決定します。通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。アダプティブプロファイルを更新すると、システムは、ネットワーク検出により検出されたホスト情報またはサードパーティからインポートしたホスト情報を使用して処理動作を調整します。

Snort 3でアダプティブプロファイルを有効にするには、**[有効化（Enable）]**オプションと**[プロファイルの更新を有効化（Enable Profile Updates）]**オプションの両方を選択する必要があります。

- **[有効化（Enable）]**：アクセス制御ルールに対してアダプティブプロファイル（デフォルト状態）を有効にし、マルウェア防御（AMP）を含むアプリケーション/ファイル制御を実行し、侵入ルールでサービスメタデータを使用します。
- **[プロファイルの更新を有効化（Enable Profile Updates）]**：ネットワーク分析ポリシーで手動で設定可能なターゲットベース プロファイルと同様に、プロファイル更新は、ターゲット ホストのオペレーティング システムと同じ方法で、IP パケットの最適化およびストリームのリアセンブルを行うのに役立ちます。その後、侵入ルールエンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。プロファイル更新は、侵入ルールのメタデータをホスト情報と比較して、特定のルールにルールを適用するかどうかを判断します。
- **[アダプティブプロファイル – 属性更新間隔（Adaptive Profiles – Attribute Update Interval）]**：プロファイル更新が有効な場合、ネットワークマップデータを管理センターからその管理対象デバイスに同期する間隔を分単位で制御できます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。このオプションの値を大きくすると、大規模なネットワークでパフォーマンスを向上させることができます。
- **[アダプティブプロファイル – ネットワーク（Adaptive Profiles – Networks）]**：プロファイル更新が有効な場合、オプションで、IPアドレス、アドレスブロック、およびネットワーク変数のカンマ区切りリストにプロファイル更新を制限することで、パフォーマンスを向上できます。ネットワーク変数を使用すると、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にリンクされている変数セットの変数の値が使用されるようになります。たとえば、192.168.1.101、192.168.4.0/24、$HOME_NET というように入力することができます。IPv4 と IPv6 がサポートされます。

  デフォルト値（0.0.0.0/0）は、すべてのネットワークにアダプティブプロファイルの更新を適用します。

パフォーマンス設定および遅延ベースのパフォーマンス設定

侵入防御のパフォーマンス チューニングについて では、侵入行為についてトラフィックを分析する際のシステムのパフォーマンスを向上させるための情報を提供しています。

遅延ベースのパフォーマンス設定固有の情報については、パケットおよび侵入ルールの遅延しきい値構成を参照してください。

暗号化された可視性エンジン

この機能の詳細については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「Encrypted Visibility Engine」の章を参照してください。

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。

⚠

注意 *Snort 2* のみ。SSL ポリシーを追加または削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックの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を参照してください。

- 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、アクセス コントロール ポリシーの詳細設定 （15 ページ）で TLS サーバー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 [編集（Edit）]（✎） をクリックします。

代わりに[表示（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。

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 アクセスコントロール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 [ヒットカウントの分析（Analyze Hit Counts）] 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、[更新（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）個々のルールで次の操作を実行できます。
  - [編集（Edit）]（）をクリックしてルールを編集します。
  - [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。
  - [スライダ（Slider）]（  ）をクリックして、ルールを有効または無効にします。
  - ルールの[X]をクリックして、ルールの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）[歯車（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[表示（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

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、ルールとその他のポリシーの警告を参照してください。

手順

ステップ 1 **[ポリシー（Policy）]** > **[アクセス制御（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。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。
- ルールの警告およびエラーを表示するには、**[分析（Analyze）]** > **[ルールの警告の表示（Show Rule 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。

- 警告とエラーは、[ルールの競合（Rule Conflicts）] とは別のタブに表示されます。
- 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 [その他（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。
- 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**。
- 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）].

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 *1*:

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
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。
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**。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
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。
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（ベータ版）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	最小 Firewall Management Center	最小 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。