アクセス コントロール ポリシーの開始

ここでは、アクセス コントロール ポリシーの使用を開始する方法について説明します。

アクセス制御の概要

アクセス制御は、（非高速パスを通る）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ベースの機能です。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、これはマルチドメイン展開で特に有用です。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。各管理対象デバイスは 1 つのアクセス コントロール ポリシーのターゲットにすることができます。

ポリシーのターゲット デバイスがネットワーク 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

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ラックリスト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。

展開のライセンスを取得せずにシステムを設定することはできますが、多くの機能では、展開する前に適切なライセンスを有効にする必要があります。また、一部の機能は、特定のデバイスモデルでのみ使用できます。サポートされていない機能は、警告アイコンおよび確認ダイアログ ボックスに示されます。

（注） システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。場合によっては、タップ モードのインラインデバイスを含むパッシブに展開されたデバイスにインライン設定を展開することがシステムによって阻害されます。それ以外の場合、ポリシーは正常に展開されますが、パッシブに展開されたデバイスを使用してトラフィックのブロックや変更を試みると、予期しない結果になる可能性があります。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

アクセス コントロール ポリシーのコンポーネント

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。

次のリストに、簡単なポリシーの作成後に変更可能な設定を示します。

（注） 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。

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。これはマルチドメイン導入環境で特に有効です。

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。1つのデバイスに適用されるアクセス コントロール ポリシーは 1 つのみです。マルチドメイン導入環境では、1 ドメイン内のすべてのデバイスで同じ基本ポリシーを使用させることができます。

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ラックリストに登録（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、ブラックリストはカスタム ホワイトリストで上書きできます。

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。ユーザに警告するページを表示するものの、ユーザ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。

関連トピック

ルール管理：共通の特性

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

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。

- インテリジェント アプリケーション バイパスで信頼されないトラフィック
- セキュリティ インテリジェンスによってブラックリスト登録されていないトラフィック
- SSL インスペクションによってブロックされていないトラフィック（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。

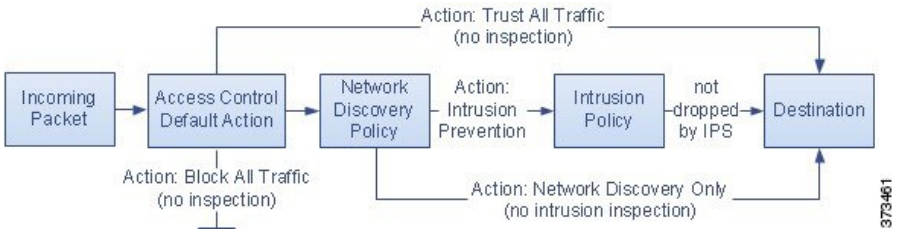
ポリシーを継承している場合、最下位の子孫のデフォルト アクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは基本ポリシーから継承することもできますが、継承したデフォルト アクションを強制的に実施することはできません。

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	インスペクションのタイプとポリシー
Access Control: Block All Traffic	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
Access Control: Trust All Traffic	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
Intrusion Prevention	ユーザ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、および 検出（discovery）、ネットワーク検出ポリシーを使用
ネットワーク検出のみ（Network Discovery Only）	許可（allow）	検出のみ（discovery only）、ネットワーク検出ポリシーを使用
基本ポリシーから継承	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 [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。

関連トピック

限定的な導入のパフォーマンスに関する考慮事項
ポリシーのデフォルト アクションによる接続のロギング

アクセス コントロール ポリシーの継承

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ブラックリストおよびホワイトリストに登録します。
- HTTP 応答ページ：ユーザの 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。

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

アクセス制御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 Firepower 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。

関連トピック

アクセス コントロール ポリシーの継承の管理 （12 ページ）
セキュリティ インテリジェンス ブラックリスト
HTTP 応答ページとインタラクティブなブロッキング
アクセス コントロール ポリシーの詳細設定 （17 ページ）
アクセス コントロール ポリシーのロギング設定 （17 ページ）

アクセス コントロール ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Access Admin Network Admin

Firepower システムでは、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。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。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

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

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。

- コピー：コピー アイコン（  ）をクリックします。
- 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 （9 ページ）を参照してください。
- 削除：削除アイコン（  ）をクリックします。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 を参照）。
- 編集：編集アイコン（  ）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 （10 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アイコン（  ）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。
- インポート/エクスポート：[インポート/エクスポート（Import/Export）] をクリックします。コンフィギュレーションのインポートとエクスポートを参照してください。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成 を参照）。

関連トピック

失効ポリシー

基本的なアクセス コントロール ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

新規アクセス コントロール ポリシーを作成する場合は、少なくとも、デフォルト アクションを選択する必要があります。

ほとんどの場合、デフォルトアクションにより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。例外は、マルチドメイン導入でサブポリシーを作成する場合です。この場合、継承されたデフォルト アクションのロギング設定に応じて、接続のロギングが有効になります。

ステップ 1 **[Policies]** > **[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。

ステップ 5 初期デフォルト アクションを指定します。

- 基本ポリシーを選択すると、新しいポリシーではそのデフォルト アクションが継承されます。ここで変更することはできません。
- [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。

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。

次のタスク

- 必要に応じて、アクセス コントロール ポリシーの編集 （10 ページ）の説明に従って、さらに新しいポリシーを設定します。
- 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。

関連トピック

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 （4 ページ）
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 （16 ページ）

アクセス コントロール ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

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。

ステップ 1 **[Policies]** > **[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アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、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。

- 名前と説明：いずれかのフィールドをクリックし、新しい情報を入力します。
- 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変数セット：[侵入防御（Intrusion Prevention）] のデフォルトアクションに関連付けられている変数セットを変更するには、変数アイコン（  ）をクリックします。表示されるポップアップ ウィンドウで、新しい変数セットを選択して [OK] をクリックします。また、編集アイコン（  ）をクリックして、選択した変数セットを新しいウィンドウで編集することもできます。詳細については、変数の管理を参照してください。
- デフォルトアクションのロギング：デフォルトアクションで処理される接続のロギングを設定するには、ロギング アイコン（  ）をクリックします。ポリシーのデフォルト アクションによる接続のロギングを参照してください。
- HTTP 応答：システムが Web サイトの要求をブロックする際にブラウザに表示される情報を指定するには、[HTTP 応答（HTTP Responses）] タブをクリックします。HTTP 応答ページの選択を参照してください。
- 継承：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、[継承設定（Inheritance Settings）] をクリックします。基本アクセス コントロール ポリシーの選択 （13 ページ）を参照してください。
- 継承：子孫での設定のロック：このポリシーの設定を子孫ポリシーに適用するには、[継承設定（Inheritance Settings）] をクリックします。子孫アクセス コントロール ポリシーのロックの設定 （14 ページ）を参照してください。
- ポリシー割り当て：ターゲット：このポリシーの対象となっている管理対象デバイスを特定するには、[ポリシー割り当て（Policy Assignment）] をクリックします。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 （16 ページ）を参照してください。
- ポリシー割り当て：ドメインで必須：このポリシーをサブドメインに適用するには、[ポリシー割り当て（Policy Assignment）] をクリックします。ドメインでのアクセス コントロール ポリシーの強制 （15 ページ）を参照してください。
- ルール：アクセス コントロール ルールを管理し、侵入とファイル 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（Rules）] タブをクリックします。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。
- ルールの競合：ルールの競合の警告を表示するには、[ルールの競合の表示（Show rule conflicts）] を有効にします。ルールの競合は、より古いルールが先にトラフィックに一致することが原因で、ルールがトラフィックに一致することがない場合に発生します。ルールの競合を判別するには多くのリソースを消費するため、それらを表示するには時間がかかることがあります。詳細については、ルールの順序指定のガイドラインを参照してください。
- セキュリティ インテリジェンス：最新のレピュテーション インテリジェンスに基づいてすぐに接続をブラックリストに載せる（ブロックする）には、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。セキュリティ インテリジェンスの設定を参照してください。
- 詳細オプション：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するには、[詳細（Advanced）] タブをクリックします。アクセス コントロール ポリシーの詳細設定 （17 ページ）を参照してください。

- 警告：アクセス コントロール ポリシー（およびその子孫ポリシーと関連ポリシー）の警告またはエラーのリストを表示するには、[警告の表示（Show Warnings）] をクリックします。警告とエラーによって、トラフィック分析やフローに悪影響を及ぼしたり、ポリシーの展開を妨げたりする構成がマークされます。警告がない場合、ボタンは表示されません。ルールの競合の警告を表示するには、まず、[ルールの競合の表示（Show rule conflicts）] を有効にします。

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。

関連トピック

ルールとその他のポリシーの警告
ディープ インスペクションについて

アクセス コントロール ポリシーの継承の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

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 （10 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、[継承設定（Inheritance Settings）] をクリックして、基本アクセス コントロール ポリシーの選択 （13 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、[継承設定（Inheritance Settings）] をクリックして、子孫アクセス コントロール ポリシーのロックの設定 （14 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、[ポリシーの割り当て（Policy Assignment）] をクリックして、ドメインでのアクセス コントロール ポリシーの強制 （15 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）] タブ、[HTTP 応答（HTTP Responses）] タブ、

または[詳細（Advanced）]タブをクリックして、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 （13 ページ）で説明する手順を実行します。

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。

基本アクセス コントロール ポリシーの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

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。

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、[継承設定（Inheritance Settings）] をクリックします。

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。

マルチドメイン展開では、アクセス コントロール ポリシーが既存のドメインで必要になることがあります。基本ポリシーとして、強制ポリシーまたはその子孫ポリシーの一つを選択できます。

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。

基本ポリシーからのアクセス コントロール ポリシー設定の継承

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

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。

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）] タブ、[HTTP 応答（HTTP Responses）] タブまたは [詳細（Advanced）] タブをクリックします。

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 ポリシーのロックの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

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。

ステップ 1 アクセス コントロール ポリシー エディタで、[設定の継承（Inheritance Settings）] をクリックします。

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

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

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。

始める前に

- 少なくとも 1 つのグローバル ドメイン以外のドメインを設定します。

ステップ 1 アクセス コントロール ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

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

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アイコン（）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。クリア アイコン（）をクリックして、検索をクリアします。

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

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

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。マルチドメイン展開では、ドメイン内のすべてのデバイスが同一の基本ポリシーを使用するように強制できます。

ステップ 1 アクセス コントロール ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 [ターゲット デバイス（Targeted Devices）] タブで、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アイコン（）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。クリアアイコン（）をクリックして、検索をクリアします。

[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 必要に応じて、[ドメインで強制（Required on Domains）] タブをクリックして、選択したサブドメイン内のすべてのデバイスが同じ基本ポリシーを使用するように強制します。ドメインでのアクセス コントロール ポリシーの強制 （15 ページ）を参照してください。

ステップ 4 [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 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 ポリシーのロギング設定

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 の宛先と syslog アラートを設定できます。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。

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、Syslog アラート応答の作成 の手順を使用して設定したとおりに、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、侵入 syslog アラートの重大度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。

[FTD 6.3 以降：デバイスに展開されている FTD プラットフォーム設定のポリシーで設定されている syslog 設定を使用（FTD 6.3 and later: 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、重大度を選択すると、接続イベントまたは侵入イベントが選択した重大度で [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、Firepower Threat Defense デバイス 6.3 以降のみに適用されます。

（注） 両方のオプションを選択すると、オプションの動作が変更されます。[ダイナミック サマリ（Dynamic Summary）] セクションに、選択の結果が表示されます。

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

アクセス コントロール ポリシーの詳細設定

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。侵入ルールの更新 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。

代わりに表示アイコン（  ）が表示される場合、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。 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。

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。

全般設定

ユーザが要求した各 URL に対して保存する文字数をカスタマイズするには、長い URL のロギングの制限を参照してください。

ユーザ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 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 ミス ルックアップを再試行する（Retry URL cache miss lookup）] を無効にすると、カテゴリがキャッシュされない場合には、クラウドルックアップを使用せずに、すぐにトラフィックが URL に渡されるようにすることができます。クラウド ルックアップで別のカテゴリが用意されるまで、クラウドルックアップを必要とする URL は未分類の URL として処理されます。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。

[Enable Threat Intelligence Director] 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。TID の詳細については、Cisco Threat Intelligence Director（TID）を参照してください。

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® の再起動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（SSL、ID、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 （20 ページ）を参照してください。

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。

- システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、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と関連付けられている変数セットの変更。
- 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/侵入ポリシーのための高度なアクセス制御の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 Firepower 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、Threat Defense 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

ファイルとマルウェアのインスペクション パフォーマンスとストレージの調整 に、ファイル制御と ネットワーク向け AMP 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。

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/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開す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。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。詳細については、トランスポート/ネットワーク プリプロセッサの詳細設定を参照してください。

検出拡張の設定

検出拡張の詳細設定では、次のことを実行できるようにアダプティブプロファイルを設定することができます。

- アクセス コントロール ルールでファイル ポリシーとアプリケーションを使用する。
- 侵入ルールでサービス メタデータを使用する。
- パッシブ展開で、ネットワークのホスト オペレーティング システムに基づいてパケット フラグメントと TCP ストリームのリアセンブルを向上させる。

詳細については、適応型プロファイルを参照してください。

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。

アクセス制御への他のポリシーの関連付け

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	機能に応じて異なる	機能に応じて異なる	いずれか（Any）	Admin/Access Admin/Network Admin

次のサブポリシーのいずれかとアクセス コントロール ポリシーとを関連付けるには、アクセス コントロール ポリシーの詳細設定を使用します。

- SSL 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、復号化、ブロック、または許可します。

  注意 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、ユーザ認証を実行します。

- 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。

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 適切な [ポリシー設定（Policy Settings）] 領域の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、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。 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。

関連トピック

Snort® の再起動シナリオ

ポリシー ヒット カウントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	Firepower Threat Defense	任意（Any）	管理/アクセス Admin/Network Admin

ヒット カウントは、一致する接続に対してポリシー ルールがトリガーされた回数を示します。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、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。サポート対象のポリシーの場合、ポリシーに設定されているデフォルト アクションのヒットカウント情報も表示されます。

（注）
- Firepower Threat Defense デバイスを再起動すると、すべてのヒット カウント情報がリセットされます。
- 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。

ステップ 1 アクセス制御またはプレフィルタ ポリシーのページに移動します。

ステップ 2 ヒット カウント情報を表示するポリシーをクリックします。

ステップ 3 ポリシーのページで、そのページの右上にある [ヒット カウントの分析（Analyze Hit Counts）] ボタンをクリックします。

ステップ 4 [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。

（注） 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 5 ヒット カウント データを取得するには、[現在のヒット カウントの取得（Fetch Current Hit Count）] ボタンをクリックします。

選択したデバイスのヒット カウント情報にアクセスしようとしたのが初めてではない場合、[現在のヒット カウントの取得（Fetch Current Hit Count）] ではなく、[更新（Refresh）] ボタンが表示されます。最新のヒット カウント情報を取得するには、[更新（Refresh）] ボタンをクリックします。

ステップ 6 （オプション）テーブルとテーブル内のリストをカスタマイズするには、[ルール/ポリシーのフィルタ処理（Filter Rules/Policy）] ボックスか、または [フィルタ条件（Filter by）] と [過去（In Last）] ドロップダウン ボックスおよび設定アイコン（⚙）を使用します。

ステップ 7 （オプション）ルール名をクリックして編集するか、最後の列の表示アイコン（🔍）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。

（注） [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。

ステップ 8 （オプション）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します。

複数のルールのヒット カウント情報をクリアするには、**Ctrl** ボタンを使用してルールを選択し、選択したルールのいずれかを右クリックした後に [ヒットカウントのクリア（Clear Hit Count）] を選択します。

（注） ヒット カウント情報をクリアすると、ヒット カウントが元のゼロに設定されます。

ステップ 9 （オプション）ページの左下にある [Generate CSV] ボタンをクリックして、詳細情報の CSV レポートをページ上で生成します。

ステップ 10 [閉じる（Close）] をクリックしてポリシー ページに戻ります。