アクセス コントロール ルール

次の各トピックでは、アクセス コントロール ルールの設定方法について説明します。

アクセス コントロール ルールの概要

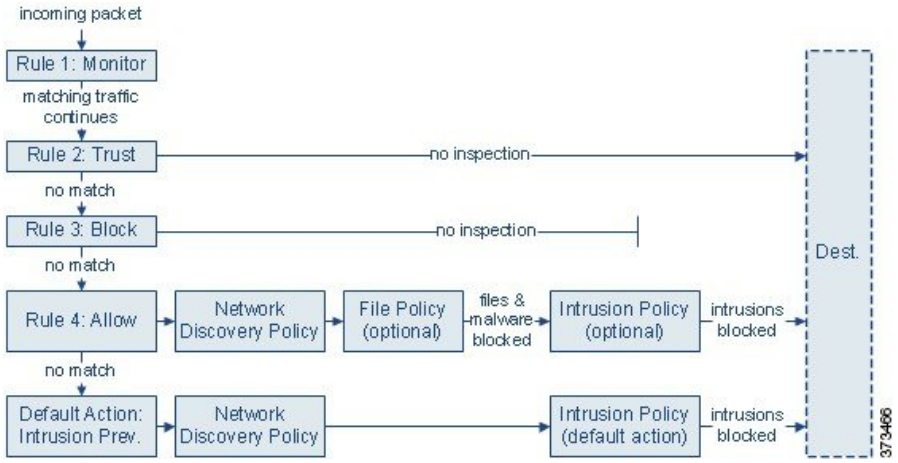
アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理するきめ細かい制御方法が提供されます。

（注） アクセス コントロール ルールがネットワーク トラフィックを評価する前に、プレフィルタ評価/8000 シリーズ高速パス、セキュリティ インテリジェンスのフィルタリング、SSL インスペクション、ユーザの識別、および一部の復号と前処理が発生します。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、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。

また、各ルールにはアクションがあり、これによって一致するトラフィックをモニタ、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

次のシナリオでは、インラインの侵入防御展開環境で、アクセス コントロール ルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1**：**モニタ**はトラフィックを最初に評価します。モニタルールはネットワークトラフィックを追跡してログに記録します。システムはトラフィックと追加ルールの照合を継続して、許可するか拒否するかを決定します（ただし、重要な例外と注意事項をアクセス コントロール ルールのモニタ アクション （13 ページ）で確認してください）。
- **ルール 2**：**信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは追加のインスペクションなしで宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。一致しなかったトラフィックは、次のルールへと進められます。
- **ルール 3**：**ブロック**はトラフィックを 3 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4**：**許可**は最後のルールです。このルールの場合、一致するトラフィックは許可されますが、そのトラフィック内の禁止されたファイル、マルウェア、侵入およびエクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない許可ルールを設定できます。
- **デフォルト アクション**はルールのいずれにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、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信頼またはブロックするデフォルト アクションが存在する場合があります。（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）。

アクセス コントロール ルールまたはデフォルトアクションによって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザデータについてネットワーク検出ポリシーによるインスペクションの対象になります。明示的に検出を有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可すると、検出データの収集は自動的に保証

されません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

暗号化されたトラフィックの通過がSSLインスペクション設定で許可される場合、またはSSLインスペクションが設定されていない場合は、そのトラフィックがアクセスコントロールルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。また、デフォルトでは、システムは暗号化されたペイロードの侵入およびファイルのインスペクションを無効にしていますこれにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

アプリケーション制御に関する推奨事項

アプリケーションによるネットワークへのアクセスを次のように制御することをお勧めします。

- 安全性の低いネットワークからより安全なネットワークへのアプリケーションアクセスを許可またはブロックするには、アクセス コントロール ルールで [ポート（Port）]（[選択した宛先ポート（Selected Destination Port）]）条件を使用します。

  たとえば、インターネット（安全性が低い）から内部ネットワーク（安全性が高い）への ICMP トラフィックを許可します。

- ユーザ グループによるアプリケーションへのアクセスを許可またはブロックするには、アクセス コントロール ルールで [アプリケーション（Application）] 条件を使用します。

  たとえば、契約業者グループのメンバーによる Facebook へのアクセスをブロックします。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

次の表に、アクセス コントロール ルールを設定する方法の例を示します。

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	Users	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポート（SSH など）を使用する場合の、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意（Any）	設定しない	使用可能なポート：**SSH** [選択した宛先ポート（Selected Destination Port）] に追加	任意（Any）	ISE/ISE-PIC でのみ使用。	任意（Any）
アプリケーションがポートを使用していない場合の（ICMP など）、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意（Any）	設定しない	選択された宛先ポート プロトコル：**ICMP** **タイプ**：**Any**	設定しない	ISE/ISE-PIC でのみ使用。	任意（Any）

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	Users	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
ユーザ グループによるアプリケーション アクセス	お客様の選択（この例では [ブロック（Block）]）	お客様の選択	ユーザ グループ（この例では契約業者グループ）を選択。	アプリケーションの名前（この例では [Facebook]）を選択。	設定しない	設定しない	ISE/ISE-PIC でのみ使用。	お客様の選択

アクセス コントロール ルールの管理

アクセス コントロール ポリシー エディタの [Rules] タブでは、現在のポリシー内のアクセス コントロール ルールの追加、編集、分類、検索、移動、有効化、無効化、削除、その他の管理が行えます。

ポリシー エディタでは、各アクセス コントロール ルールに対してルールの名前、条件の概要、ルール アクションが表示され、さらにルールのインスペクション オプションや状態を示すアイコンが表示されます。各アイコンの意味は次のとおりです。

- 侵入ポリシー オプション（  ）
- ファイル ポリシー オプション（  ）
- セーフ サーチ オプション（  ）
- YouTube EDU オプション（  ）
- ロギング オプション（  ）
- 発信元クライアント オプション（  ）
- コメント（  ）
- 警告（  ）
- エラー（  ）
- 重要な情報（  ）

無効なルールはグレー表示され、ルール名の下に [（無効）（(disabled)）] というマークが付きます。

ルールを作成または編集するには、アクセス コントロール ルール エディタを使用します。次の操作を実行できます。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。
- エディタの左下にあるタブを使用して、条件を追加します。
- インスペクションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインスペクションおよびロギングのオプションがリストされます。

（注） アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには必須なものです。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。

関連トピック

アクセス コントロール ルールのコンポーネント （6 ページ）
カスタム ユーザ ロールの作成
ルールのパフォーマンスに関するガイドライン

アクセス コントロール ルールのコンポーネント

一意の名前に加え、各アクセス コントロール ルールには次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。ポリシー継承を使用する場合、ルール 1 は再外部ポリシーの 1 番目のルールです。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

また、ルールはセクションおよびカテゴリに属していることがあります。これは、単に整理のためであり、ルールの位置に影響しません。ルールの位置は、すべてのセクションとカテゴリにまたがって設定されます。

セクションおよびカテゴリ

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。アクセス コントロール ルールをさらに細かく整理するため、「必須（Mandatory）」セクション内と「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」セクションと「デフォルト（Default）」セクションの間にネストされます。

条件

条件は、ルールで処理する特定のトラフィックを指定します。条件は単純または複雑にできます。条件の使用はライセンスによって異なります。

Action

ルールのアクションは、一致したトラフィックの処理方法を決定します。一致するトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。信頼できるトラフィック、ブロックされたトラフィック、または暗号化されたトラフィックに対しては、詳細な検査は実行**されません**。

インスペクション（Inspection）

詳細検査オプションは、悪意のあるトラフィックをどのように検査してブロックし、それ以外のものは許可するかを決定します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ロギング

ルールのロギング設定は、システムが処理するトラフィックのレコードの維持を制御します。各ルールに一致したトラフィックのレコードを維持できます。一般的に、接続の開始時または終了時（あるいは、その両方）にセッションをログに記録できます。接続のログは、データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

説明

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。

関連トピック

ルールのパフォーマンスに関するガイドライン
アクセス コントロール ルールの管理 （5 ページ）
アクセス コントロール ルールの作成および編集 （10 ページ）
ルール条件タイプ
アクセス コントロール ルールのアクション （13 ページ）

ディープ インスペクションについて
接続のロギングのベスト プラクティス
アクセス コントロール ルールのコメント （16 ページ）

アクセス コントロール ルールの順序

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、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。モニタルールを除いて、トラフィックがルールに一致した後、システムは優先度の低い追加のルールに対してトラフィックの評価は続行しません。

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。さらに細かく整理するため、「必須（Mandatory）」セクション内や「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」ルール セクションと「デフォルト（Default）」ルール セクションの間にネストされます。ルール 1 は、現在のポリシーではなく、最外部ポリシーの 1 番目のルールです。ルールの番号は、すべてのポリシー、セクション、カテゴリにまたがって割り当てられます。

アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールによって、ルールのカテゴリ内またはカテゴリ間でアクセス コントロール ルールを移動および変更することもできます。しかし、ユーザがルールを移動および変更することを制限するには、カスタム ロールを作成できます。アクセス コントロール ポリシーの変更権限が割り当てられているユーザは、制限なく、カスタム カテゴリにルールを追加することや、カテゴリ内のルールを変更することができます。

ヒント アクセス コントロール ルールの順序を適切にすることで、ネットワーク トラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

関連トピック

ルールの順序指定のガイドライン

アクセス制御ルール カテゴリの追加

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 ポリシーの必須ルールセクションとデフォルトルールセクションをカスタムカテゴリに分割できます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ステップ 1 アクセス コントロール ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入（Insert new category）] を選択することもできます。

ステップ 2 名前を入力します。

ステップ 3 [挿入（Insert）] ドロップダウン リストから、カテゴリを追加する先を選択します。

- カテゴリをセクションのすべての既存カテゴリの下に挿入するには、[必須ルール内（Into Mandatory）] または [デフォルトルール内（into Default）] を選択します。
- 既存のカテゴリの上に挿入するには、[カテゴリの上（above category）] を選択した後、カテゴリを選択します。
- アクセス制御ルールの上または下に挿入するには、[ルールの上（above rule）] または [ルールの下（below rule）] を選択した後、既存のルール番号を入力します。

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 ルールの作成および編集

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

ステップ 1 アクセス コントロール ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 [Name] を入力します。

ステップ 3 ルール コンポーネントを設定するか、またはデフォルトを受け入れます。

- [有効（Enabled）]：ルールを有効にするかどうかを指定します。
- [位置（Position）]：ルールの位置を指定します。アクセス コントロール ルールの順序 （8 ページ）を参照してください。
- [アクション（Action）]：ルールの [アクション（Action）] を選択します。アクセス コントロール ルールのアクション （13 ページ）を参照してください。
- [条件（Conditions）]：追加する条件に対応するタブをクリックします。詳細は、ルール条件タイプを参照してください。
- [ディープ インスペクション（Deep Inspection）]：許可ルールおよびインタラクティブ ブロック ルールの場合、侵入調査アイコン（  ）またはファイルおよびマルウェア調査アイコン（  ）をクリックして、ルールの [インスペクション（Inspection）] オプションを設定します。アイコンが淡色表示の場合、そのタイプのポリシーがルールに選択されていません。詳細については、侵入ポリシーとファイル ポリシーを使用したアクセス制御を参照してください。
- [コンテンツの制限（Content Restriction）]：セーフ サーチ アイコン（  ）または YouTube EDU アイコン（  ）をクリックして、ルール エディタの [アプリケーション（Applications）] タブでコンテンツ制限設定を行います。アイコンが淡色表示の場合、ルールに対してコンテンツ制限は無効になっています。詳細については、コンテンツ制限についてを参照してください。
- [ロギング（Logging）]：アクティブな（青の）ロギング アイコン（  ）をクリックして、[ロギング（Logging）] オプションを指定します。アイコンが淡色表示の場合、接続ロギングがそのルールで無効になっています。詳細については、接続のロギングのベスト プラクティスを参照してください。

- [コメント（Comments）]：コメント列の数字をクリックして、[コメント（Comments）] を追加します。数字は、ルールにすでに含まれているコメントの数を示します。詳細については、アクセス コントロール ルールのコメント （16 ページ）を参照してください。

ステップ 4 ルールを保存します。

ステップ 5 [保存（Save）] をクリックして、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

ルールのパフォーマンスに関するガイドライン

アクセス コントロール ルールの有効化と無効化

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 ルールを作成すると、デフォルトで有効になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールについての警告とエラーが停止されます。アクセス コントロール ポリシーでルールのリストを表示するとき、無効状態のルールはグレーで表示されますが、変更は可能です。

ヒント また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。

ステップ 1 アクセス コントロール ポリシー エディタで、ルールを右クリックし、ルールの状態を選択します。

代わりに表示アイコン（）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 **[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

アクセス コントロール ルールのコンポーネント （6 ページ）

アクセス コントロール ルールの配置

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

既存のルールは、アクセス コントロール ポリシー内で移動できますが、アクセス コントロール ポリシー間では移動できません。カテゴリにルールを追加または移動すると、そのルールはシステムによってカテゴリの最後に配置されます。

ヒント 複数のルールを一度に移動するには、移動するルールを選択し、右クリック メニューを使用してカット アンド ペーストします。

ステップ 1 アクセス制御ルール エディタには、次のオプションがあります。

- 新しいルールを追加する場合は、[挿入（Insert）] ドロップダウンリストを使用します。
- 既存のルールを編集する場合、[移動（Move）] をクリックします。

ステップ 2 ルールを移動またはルールを挿入する場所を選択します。

- [必須に挿入（into Mandatory）] または [デフォルトに挿入（into Default）] を選択します。
- [カテゴリに挿入（into Category）] を選択して、ユーザ定義カテゴリを選択します。
- [ルールの上（above rule）] または [ルールの下（below rule）] を選択してから、適切なルール番号を入力します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [保存（Save）] をクリックして、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 ルールのアクション

アクセス コントロール ルールには、システムが一致するトラフィックをどのように処理し、ロギングするのかを指定するアクションがあります。モニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

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、モニタ以外のアクションをもつどのアクセスコントロールルールの条件にも一致しないトラフィックを処理します。

アクセス コントロール ルールのモニタ アクション

[Monitor] アクションは、トラフィックを許可または拒否するように設計されていません。むしろ、その主な目的は、一致するトラフィックが最終的にどのように処理されるかに関係なく、接続ロギングを強制することです。

接続がモニタルールに一致する場合、接続が一致する次の非モニタルールがトラフィック処理とそれ以降のインスペクションを決定する必要があります。さらに一致するルールがない場合、システムはデフォルトアクションを使用する必要があります。

ただし、例外があります。モニタルールにレイヤ7の条件（アプリケーション条件など）が含まれている場合、そのシステムでは早期パケットを通過させ、接続を確立（またはSSLハンドシェイクの完了）することができます。これは、接続が後続のルールによってブロックされる必要がある場合でも発生します。これらの早期パケットが後続のルールに対して評価されないためです。こうしたパケットが完全に検査されていない宛先に到達しないように、アクセスコントロールポリシーのデフォルト侵入ポリシーによって検査されます。デフォルトの侵入ポリシーを参照してください。システムはレイヤ 7 の識別を完了した後、残りのセッショントラフィックに適切なアクションを適用します。

注意 ベストプラクティスとして、広範に定義されたモニタルールのレイヤ7の条件をルールの優先順位内で高く設定しないようにすることで、不注意でトラフィックがネットワークに流入することを防ぎます。さらに、ローカルでバインドされているトラフィックがレイヤ3展開のモニタルールに一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で [Inspect Local Router Traffic] を有効にします。

関連トピック

モニタされた監視接続のロギング

アクセス コントロール ルールの信頼アクション

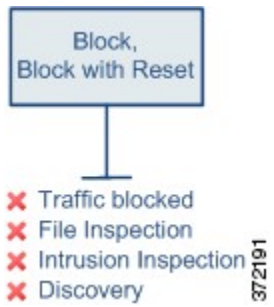
[信頼（Trust）] アクションは、ディープ インスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼処理されたトラフィックも、ID 条件およびレート制限の対象です。

関連トピック

信頼されている接続のロギング

アクセス コントロール ルールのブロック アクション

ブロック アクションおよび**リセットしてブロック** アクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。



[HTTP 応答（HTTP response）] ページに一致する Web 要求を除き、リセット ルールを持つブロックが接続をリセットします。これは、システムが Web 要求をブロックするときに表示されるように設定した応答ページは、接続がすぐにリセットされた場合は表示できないためです。詳細については、「HTTP 応答ページとインタラクティブなブロッキング」を参照してください。

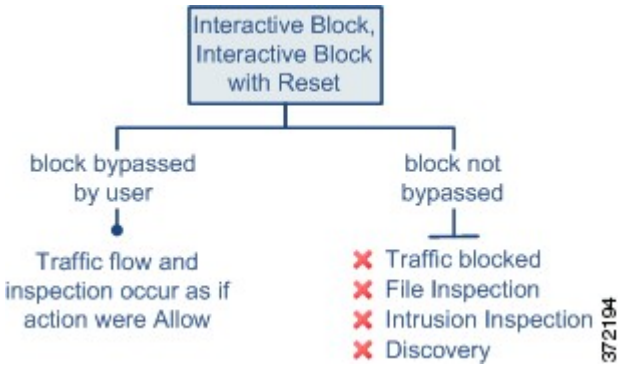
関連トピック

ブロックされた接続のロギング

HTTP 応答ページについて

アクセス コントロール ルール インタラクティブ ブロック アクション

詳細については、HTTP 応答ページとインタラクティブなブロッキングを参照してください。



ユーザがブロックをバイパスしている場合、ルールは許可ルールを模倣します。したがって、インタラクティブ ブロック ルールをファイル ポリシーと侵入ポリシーに関連付けることができるため、一致するトラフィックもネットワーク検出の対象となります。

ユーザがブロックをバイパスしない（できない）場合は、ルールはブロック ルールを模倣します。一致するトラフィックは、追加のインスペクションなしで拒否されます。

インタラクティブブロックを有効にした場合は、ブロックされているすべての接続をリセットできません。これは、接続がすぐにリセットされた場合は応答ページを表示できないためです。[リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを（非インタラクティブに）Web 以外のすべてのトラフィックをリセットしてブロックしても、Web 要求についてはインタラクティブ ブロックは有効になっています。

詳細については、HTTP 応答ページとインタラクティブなブロッキングを参照してください。

関連トピック

許可された接続のロギング

TLS/SSL ルールのブロック アクション

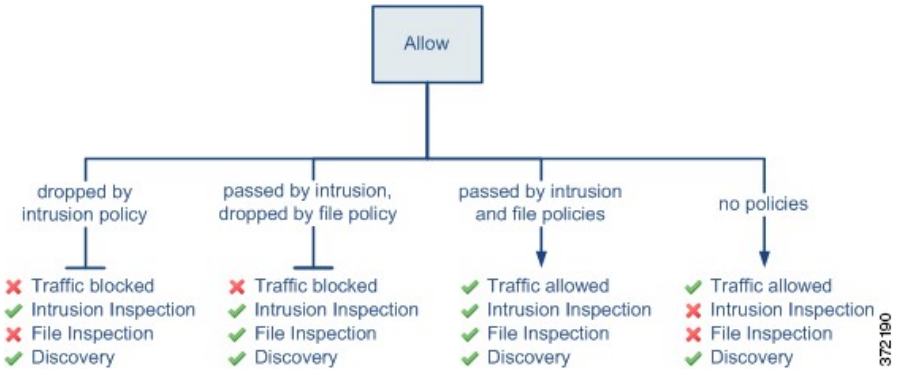
アクセス コントロール ルールの許可アクション

[許可（Allow）] アクションは、一致するトラフィックを通過させます。ただし、引き続き ID 条件およびレート制限の対象となります。

任意で、ディープインスペクションを行い、トラフィックが接続先に到達する前に暗号化されていないトラフィックや復号されたトラフィックを検査、ブロックすることも可能です。

- 侵入ポリシーでは、侵入検知と防御設定に応じてネットワーク トラフィックを分析し、設定内容に応じて違反パケットをドロップすることが可能です。
- ファイル ポリシーでは、ファイルの制御ができます。ファイル制御により、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- ネットワークベースの高度なマルウェア保護（AMP）もファイル ポリシーを使用して実行できます。ネットワーク向け AMP はファイルのマルウェアを調べ、検出したマルウェアを設定に応じてブロックします。

下の図は、許可ルールの条件（またはユーザによりバイパスされるインタラクティブブロック ルール）を満たすトラフィックに対して実行されるインスペクションの種類を示しています。侵入インスペクションの前にファイルインスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連のエクスプロイトについては検査されません。



単純化のために、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを図に示しています。ただし、いずれか一方を設定して他方は設定なしにすることもできます。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決定されます。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決定されます。

トラフィックが侵入ポリシーとファイルポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可することは検出インスペクションが自動的に保証されることではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

関連トピック

許可された接続のロギング

アクセス コントロール ルールのコメント

アクセス コントロール ルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

関連トピック

アクセス コントロール ポリシーの設定の構成

アクセス制御ルールへのコメントの追加

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 アクセス コントロール ルール エディタで、[コメント（Comments）] タブをクリックします。

ステップ 2 [New Comment] をクリックします。

ステップ 3 コメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [保存（Save）] をクリックして、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。