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

次の各トピックでは、侵入ポリシーとファイルポリシーを使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

ディープ インスペクションについて

侵入ポリシーとファイルポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイル ポリシーは、システムのファイル制御と ネットワーク向け AMP の機能を管理します。

アクセス コントロールはディープ インスペクションの前に発生し、アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。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。

システムは、AMP クラウドからエンドポイント向け AMP データを受信し、このデータを任意の ネットワーク向け AMP データと一緒に表示できます。

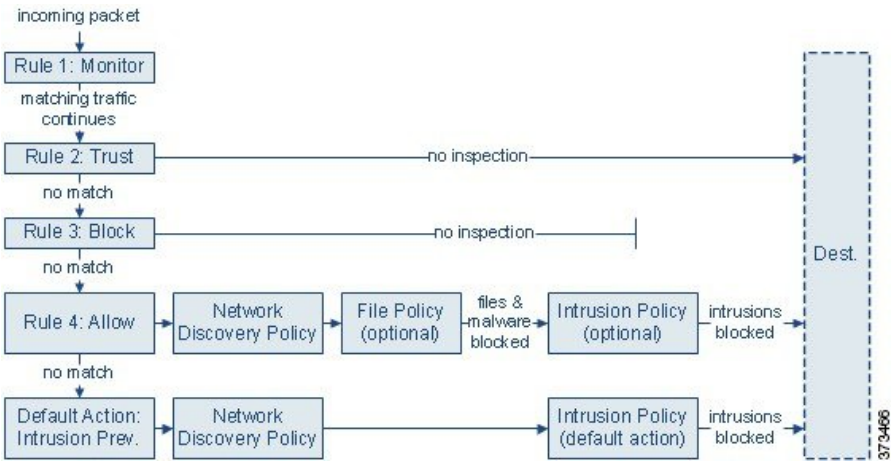
関連トピック

ポリシーが侵入についてトラフィックを検査する仕組み
ファイル ポリシー

アクセス コントロール トラフィック処理

アクセス コントロール ルールは、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詳細な方法を提供します。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。アクセス コントロール ルールのアクションによって、システムが一致するトラフィックをどのように処理するかが決まります。一致した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）できます。

次の図は、4 つの異なるタイプのアクセス コントロール ルールとデフォルト アクションを含むアクセス コントロール ポリシーによって制御されている、インラインの侵入防御と ネットワーク向け AMP の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の 3 つのアクセス コントロール ルール（モニタ、信頼およびブロック）は一致するトラフィックを検査できません。モニタ ルールはネットワーク トラフィックの追跡とロギングを行いますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。信頼ルールおよびブロック ルール

は、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセス コントロール ルールに照合されます。

ポリシー内の4番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **ディスカバリ**：**ネットワーク検出ポリシー**：最初に、ネットワーク検出ポリシーがトラフィックのディスカバリ データの有無を検査します。検出はパッシブ分析で、トラフィックのフローに影響しません。検出は明示的には有効にしませんが、拡張したり無効にしたりすることができます。ただし、トラフィックを許可することで、検出データの収集が自動的に保証されるものではありません。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、検出を実行します。
- **ネットワーク向け AMP とファイル制御**：**ファイル ポリシー**：システムは、トラフィックがディスカバリによって検査された後、トラフィックの禁止ファイルやマルウェアを検査できます。ネットワーク向けAMPは、PDF、Microsoft Officeドキュメントなど多数のファイル タイプに潜むマルウェアを検出し、オプションでブロックできます。部門がマルウェア ファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により、特定のファイル タイプの伝送についてネットワーク トラフィックをモニタし、ファイルをブロックまたは許可できます。
- **侵入防御**：**侵入ポリシー**：ファイルインスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映できます。
- **接続先**：前述のすべてのチェックを通過したトラフィックは、その接続先に渡されます。

インタラクティブ ブロック ルール（この図には表示されていません）には、許可ルールと同じインスペクション オプションがあります。これにより、あるユーザが警告ページをクリックスルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。

ポリシー内のモニタ以外のアクセス コントロール ルールのいずれにも一致しないトラフィックは、デフォルト アクションによって処理されます。このシナリオでは、デフォルト アクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終宛先に許可されます。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 アクションが割り当てられている場合もあります。システムはデフォルト アクションによって許可されたトラフィックに対し検出データおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

（注） 場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

ファイルインスペクションおよび侵入インスペクションの順序

アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイル ポリシーに関連付けて、インスペクション プロファイルをさまざまなタイプのトラフィックに照合できます。

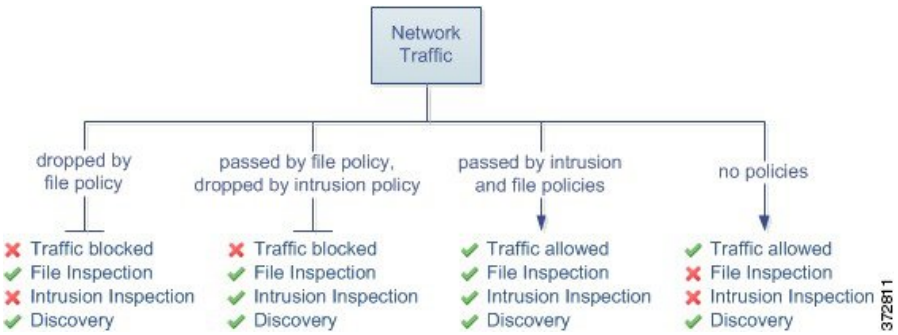
（注） 侵入防御またはネットワーク検出のみのデフォルトアクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイルインスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- 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まります
- 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まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます

ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイルポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、許可アクセス コントロール ルール、またはユーザによりバイパスされたインタラクティブ ブロック アクセス コントロール ルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。



アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイルインスペクション内では、タイプによる単純なブロッキングの方が、マルウェアインスペクションおよびブロッキングよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF も検査およびブロックします。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェア インスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェアの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

（注） ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

ファイル制御およびマルウェア保護のためのアクセスコントロール ルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイル ポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを Firepower Management Center データベースに自動的にロギングします。ログファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。

また、システムは、呼び出し元のアクセス コントロール ルールのロギング設定にかかわらず、関連付けられた接続の終了を Firepower Management Center データベースにロギングします。

ファイル制御および AMP を実行するアクセス コントロール ルールの設定

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	サポートされるドメイン	アクセス（**Access**）
脅威（ファイル制御） マルウェア（AMP）	保護（ファイル制御） マルウェア（AMP）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

⚠

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化/無効化した場合、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除した場合には、設定の変更を展開すると 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。詳細については、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。

始める前に

- AMP を含むファイル制御をアクセス コントロール ルールで実行するためには、適応型プロファイルの設定 で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする**必要があります**。

手順

ステップ 1 アクセス コントロール ルール エディタで、[許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] の [アクション（Action）] を選択します。

ステップ 2 [インスペクション（Inspection）] タブをクリックします。

ステップ 3 アクセスコントロールルールに一致するトラフィックを検査する場合は[マルウェア ポリシー（Malware Policy）]（ファイル ポリシー）を選択し、または一致するトラフィックに対するファイル インスペクションを無効にする場合は [なし（None）] を選択します。

ステップ 4 （オプション）[ロギング（Logging）] タブをクリックし、[ログ ファイル（Log Files）] チェックボックスをオフにして、一致する接続のファイルまたはマルウェア イベントのロギングを無効にします。

（注） シスコでは、ファイル イベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

ステップ 5 ルールを保存します。

ステップ 6 [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

ファイル ポリシーの作成

Snort® の再起動シナリオ

侵入防御のためのアクセス コントロール ルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先のIPアドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトセットにあるデフォルトの変数を変更します。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

Firepower システムには複数の侵入ポリシーが付属しています。システム提供の侵入ポリシーを使用することで、Cisco Talos Security Intelligence and Research Group（Talos）の経験を活用できます。これらのポリシーでは、Talos が侵入ルールおよびプリプロセッサ ルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。カスタム ポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

接続イベントおよび侵入イベントのロギング

アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成し、そのイベントを Firepower Management Center に保存します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を Firepower Management Center データベースに自動的にロギングします。

関連トピック

定義済みデフォルト変数

アクセス コントロール ルールの設定と侵入ポリシー

ユーザが独自に作成するカスタム侵入ポリシーに加え、初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーがシステムで用意されています。これらの 2 つの侵入ポリシーは、ベースとして Balanced Security and Connectivity 侵入ポリシーを使用します。両者の唯一の相違点は、[インライン時にドロップ（Drop When Inline）] 設定です。インライン ポリシーではドロップ動作が有効化され、パッシブ ポリシーでは無効化されています。

1 つのアクセス コントロール ポリシーで使用可能な一意の侵入ポリシーの数は、ターゲット デバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲット デバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを展開できません。

侵入防御を実行するアクセス コントロール ルールの設定

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	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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、新しいルールを作成するか、既存のルールを編集します。アクセス コントロール ルールのコンポーネントを参照してください。

ステップ 2 ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 3 [削除 タブを選択します。

ステップ 4 システムによって提供されるまたはカスタムの**侵入ポリシー**を選択するか、またはアクセス コントロール ルールに一致するトラフィックに対する侵入インスペクションを無効にするには [なし（None）] を選択します。

ステップ 5 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット（Variable Set）] ドロップダウン リストから値を選択します。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

ステップ 7 [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

変数セット

Snort® の再起動シナリオ