



アクセスコントロールルールを使用したトラフィックフローの調整

アクセスコントロールポリシー内で、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処理する詳細な方法を提供しています。



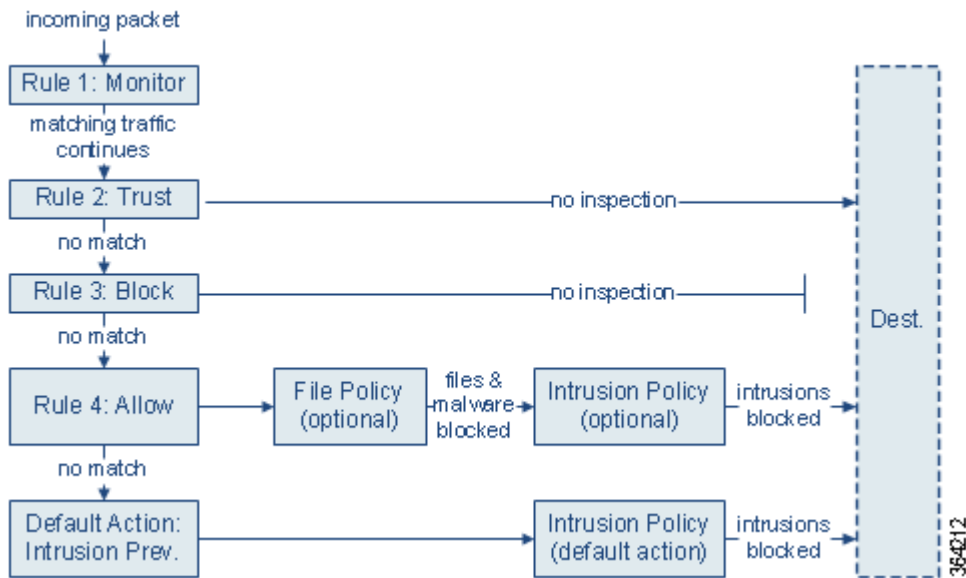
注

セキュリティインテリジェンスベースのトラフィックフィルタリング、および一部の復号化と前処理は、ネットワークトラフィックがアクセスコントロールルールによって評価される前に行われます。また、SSLインスペクション機能を設定すると、暗号化されたトラフィックをアクセスコントロールルールが評価する前にブロックしたり復号化したりできます。

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。条件は単純または複雑にできます。セキュリティゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求されたURL、およびユーザごとにトラフィックを制御できます。

各ルールにはアクションも含まれており、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定します。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。ただし、システムはトラフィックを信頼またはブロックした後は、追加のインスペクションを実行しません。

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が、トラフィックフローには影響しません。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。
- **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その宛先への通過を許可されます。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せんが、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に許可されます。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追加の許可ルールを割り当てることができることに留意してください。
- **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の詳細については、以下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\(6-3 ページ\)](#)
- [ポリシー内のアクセスコントロールルールの管理\(6-12 ページ\)](#)
- [アクセスコントロールポリシーとルールのトラブルシューティング\(4-13 ページ\)](#)

アクセスコントロールルールの作成および編集

ライセンス:すべて

アクセスコントロールポリシー内で、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処理する詳細な方法を提供しています。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。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、そのルールの場合の警告とエラーの生成が停止されます。

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。システムは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。モナルールを除き、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。

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、セキュリティゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求されたURL、またはユーザ別にトラフィックを照合できます。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。システムは、信頼されたトラフィックとブロックされたトラフィックに対してインスペクションを実行しないことに注意してください。

インスペクション

アクセスコントロールルールのインスペクションオプションは、何も行われなければユーザが許可していたであろう悪意のあるトラフィックをシステムが検査およびブロックする方法を制御します。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。一般に、接続の開始時および終了時にセッションをログに記録できます。接続のログは、ASA FirePOWER モジュールの他に、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。

注

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。

アクセスコントロールルールを追加および編集するには、アクセスコントロールルールエディタを使用します。アクセスコントロールポリシーエディタの [Rules] タブからルールエディタにアクセスします。ルールエディタで、次の操作を実行します。





- 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ブション処理したり、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。詳細については、[アクセスコントロールポリシーとルールのトラブルシューティング\(4-13 ページ\)](#)を参照してください。

アクセスコントロールルールを作成または変更するには、次の手順を実行します。

- ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy]の順に選択します。
- ステップ 2** ルールの追加先に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。
- ステップ 3** 次の選択肢があります。
- 新しいルールを追加するには、[Add Rule]をクリックします。
 - 既存のルールを編集するには、そのルールの横にある編集アイコン()をクリックします。
- ステップ 4** 規則の名前を入力します。
- 各ルールには一意の名前が必要です。30文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン(:)は使用できません。
- ステップ 5** 前述の説明に従い、ルールコンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。
- ルールを有効にするかどうか [Enabled]を指定します。
 - ルールの位置を指定します。「[ルールの評価順序の指定\(6-5 ページ\)](#)」を参照してください。
 - ルールの [Action]を選択します。ルールアクションを使用したトラフィックの処理とインスペクションの決定([6-8 ページ](#))を参照してください。
 - ルールの条件を設定します。「[ルールが処理するトラフィックを指定するための条件の使用\(6-6 ページ\)](#)」を参照してください。
 - 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は、ルールのインスペクションオプションを設定します。[侵入ポリシーおよびファイルポリシーを使用したトラフィックの制御\(11-1 ページ\)](#)を参照してください。
 - [Applications]タブでセーフサーチ()アイコンまたは YouTube EDU()アイコンをクリックして、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、[アクセスコントロールルールを使用したコンテンツ制限の実施\(12-2 ページ\)](#)を参照してください。
 - [Logging]オプションを指定します。「[ネットワークトラフィックの接続のロギング\(35-1 ページ\)](#)」を参照してください。
 - コメントを追加します。[ルールへのコメントの追加\(6-11 ページ\)](#)を参照してください。

ステップ 6 [Store FirePOWER Changes]をクリックして変更を保存します。

ルールが保存されます。削除アイコン(🗑️)をクリックすると、ルールを削除できます。変更を反映させるには、アクセスコントロールポリシーを適用する必要があります([設定変更の展開 \(4-12 ページ\)](#)を参照してください)。

ルールの評価順序の指定

ライセンス:すべて

最初にアクセスコントロールルールを作成するとき、ルールエディタで [Insert] ドロップダウンリストを使用してその位置を指定します。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。モニタールール(トラフィックをログに記録するがトラフィックフローには影響しないルール)の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。



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、ルールのプリエンブ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、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。詳細については、[パフォーマンスを向上させプリエンブションを回避するためのルールの順序付け \(4-15 ページ\)](#)を参照してください。

ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには3つのカテゴリ(管理者、標準、ルート)があります。カスタムカテゴリを追加できますが、シスコ提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。既存のルールの位置またはカテゴリの変更の詳細については、「[ルールの位置またはカテゴリの変更 \(6-14 ページ\)](#)」を参照してください。

ルールの編集や作成中にルールをカテゴリに追加する手順:

ステップ 1 アクセスコントロールルールエディタで、[Insert]ドロップダウンリストから、[Into Category]を選択し、使用するカテゴリを選択します。

ルールを保存すると、そのカテゴリの最後に配置されます。

ルールの編集や作成中にルールの位置を数値で指定する手順:

ステップ 1 アクセスコントロールルールエディタで、[Insert]ドロップダウンリストから、[above rule]または[below rule]を選択し、適切なルール番号を入力します。

ルールを保存すると、指定した位置に配置されます。

ルールが処理するトラフィックを指定するための条件の使用

ライセンス:機能によって異なる

アクセスコントロールルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は単純または複雑にできます。セキュリティゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御できます。

条件をアクセスコントロールルールに追加する場合は、次の点に注意してください。

- 1つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、特定のホストの URL フィルタリング (URL 条件) を実行する単一のルールを使用できます (ゾーンまたはネットワーク条件)。
- ルールの条件ごとに、最大 50 の基準を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、単一のルールを使用して、最大 50 のユーザおよびグループのユーザ制御を実行できます。

最大 50 の送信元の基準と最大 50 の宛先の基準を使用して、送信元と宛先ごとにゾーンおよびネットワークの条件を制約できます。送信元基準と宛先基準の両方をゾーンまたはネットワーク条件に追加する場合、一致するトラフィックは指定された送信元ゾーン/ネットワークの 1 つから発生し、宛先ゾーン/ネットワークの 1 つを通して出力する必要があります。つまり、システムは、同じタイプの複数の条件基準を **OR** 演算でリンクし、複数の条件タイプを **AND** 演算でリンクします。たとえば、次のようなルール条件の場合、

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

ルールは、プライベートな IPv4 ネットワークの 1 つでホストからのピアツーピアアプリケーショントラフィックを照合します。パケットは**いずれか一方または他の送信元ネットワーク**から発生し、ピアツーピアアプリケーショントラフィックを表す必要があります。次の接続の両方がルールをトリガーします。

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

ルールに特定の条件を設定しない場合、その条件によるトラフィック照合は行われません。たとえば、ネットワーク条件を持つがアプリケーション条件を持たないルールは、セッションで 사용되는アプリケーションに関係なく、送信元または宛先に基づいてトラフィックを評価します。



注

アクセスコントロールポリシーを適用すると、システムはすべてのルールを評価し、ネットワークトラフィックを評価するために ASA FirePOWER モジュールが使用する基準の拡張セットを作成します。複雑なアクセスコントロールポリシーおよびルールは、重要なリソースを消費する可能性があります。アクセスコントロールルールを簡素化するヒントと、パフォーマンスを改善する他の方法については、[アクセスコントロールポリシーとルールのトラブルシューティング \(4-13 ページ\)](#)を参照してください。

アクセスコントロールルールを追加または編集するときは、ルールエディタの左下にあるタブを使用してルール条件を追加および編集します。次の表に、追加できる条件のタイプを示します。

表 6-1 アクセスコントロールルール条件のタイプ

条件	トラフィックの照合	詳細
ゾーン	特定のセキュリティゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信	セキュリティゾーンは、ご使用の導入ポリシーおよびセキュリティポリシーに準じた1つ以上のインターフェイスの論理グループです。ゾーン条件を作成するには、 セキュリティゾーンによるトラフィックの制御(7-2 ページ) を参照してください。
ネットワーク	その送信元または宛先の IP アドレス、国、または大陸による	明示的に IP アドレスまたはアドレスブロックを指定できます。位置情報の機能では、送信元または宛先となる国や大陸を基準にしたトラフィック制御もできます。ネットワーク条件の作成については、「 ネットワークまたは地理的位置によるトラフィックの制御(7-3 ページ) 」を参照してください。
ポート	送信元ポートまたは宛先ポート	TCP および UDP の場合、トランスポート層プロトコルに基づいてトラフィックを制御できます。ICMP および ICMPv6 (IPv6 ICMP) の場合、インターネット層プロトコルと、オプションのタイプおよびコードに基づいてトラフィックを制御できます。ポート条件を使用して、ポートを使用しない他のプロトコルでトラフィックを制御することもできます。ポート条件の作成については、「 ポートおよび ICMP コードによるトラフィックの制御(7-5 ページ) 」を参照してください。
アプリケーション	セッションで検出されるアプリケーション	基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに応じて、個々のアプリケーションへのアクセスまたはフィルタアクセスを制御できます。アプリケーション条件の作成については、「 アプリケーショントラフィックの制御(8-2 ページ) 」を参照してください。
URL	セッションで要求された URL による	ネットワーク上のユーザが個別にまたは URL の一般的な分類とリスクレベルに基づいてアクセスできる Web サイトを制限できます。URL 条件の作成については、「 URL のブロッキング(8-8 ページ) 」を参照してください。
ユーザ	セッションに参加しているユーザ	モニタ対象セッションに参加するホストにログインした LDAP ユーザに基づいてトラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。ユーザ条件の作成については、「 アクセスコントロールルール: レルムとユーザ(9-1 ページ) 」を参照してください。

任意のライセンスを使ってアクセスコントロールルールを作成できますが、ルール条件によっては、ポリシーを適用する前に、特定のライセンス機能を有効にする必要があることに注意してください。詳細については、[アクセスコントロールのライセンス要件\(4-2 ページ\)](#)を参照してください。

ルールアクションを使用したトラフィックの処理とインスペクションの決定

ライセンス:すべて

すべてのアクセスコントロールルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- **処理:**まず第一に、ルールアクションは、システムがルールの条件に一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを制御します。
- **インスペクション:**特定のルールアクションでは、適切にライセンス付与されている場合、通過を許可する前に一致するトラフィックをさらに検査することができます。
- **ロギング:**ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

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、モニタ以外の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(デフォルトの処理の設定およびネットワークトラフィックのインスペクション(4-4 ページ)を参照)。

インラインで展開されたデバイスのみがトラフィックをブロックまたは変更できることに留意してください。パッシブに展開されたデバイスは、トラフィックのフローを分析およびログに記録できますが、影響を与えることはありません。ルールアクションの詳細と、ルールアクションがトラフィックの処理、インスペクション、およびロギングにどのように影響するかについては、次の項を参照してください。

- [モニタアクション:アクションの遅延とログの確保\(6-8 ページ\)](#)
- [信頼アクション:インスペクションなしでのトラフィックの通過\(6-9 ページ\)](#)
- [ブロッキングアクション:インスペクションなしでトラフィックをブロック\(6-9 ページ\)](#)
- [インタラクティブブロッキングアクション:ユーザがWebサイトブロックをバイパスすることを許可する\(6-10 ページ\)](#)
- [許可アクション:トラフィックの許可および検査\(6-10 ページ\)](#)
- [侵入ポリシーおよびファイルポリシーを使用したトラフィックの制御\(11-1 ページ\)](#)
- [アクセスコントロールの処理に基づく接続のロギング\(35-10 ページ\)](#)

モニタアクション:アクションの遅延とログの確保

ライセンス:すべて

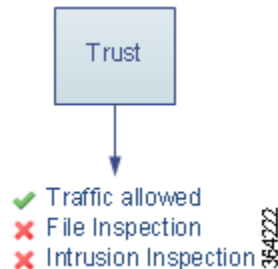
モニタアクションはトラフィックフローに影響を与えません。つまり、一致するトラフィックが直ちに許可または拒否されることはありません。その代わりに、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタルール以外の一致する最初のルールが、トラフィックフローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルトアクションを使用します。

モニタルールの主な目的はネットワークトラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、トラフィックが他のルールに一致せず、デフォルトアクションでロギングが有効になっていない場合でも、接続はログに記録されます。詳細については、[モニタされる接続のロギングについて\(35-5 ページ\)](#)を参照してください。

信頼アクション:インスペクションなしでのトラフィックの通過

ライセンス:すべて

信頼アクションでは、トラフィックはいかなる種類の追加のインスペクションなしで通過を許可されます。

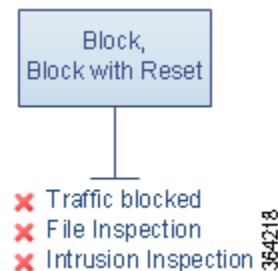


信頼されたネットワークトラフィックは、接続の開始および終了の両方でログに記録できます。詳細については、[信頼されている接続のログギングについて \(35-5 ページ\)](#)を参照してください。

ブロッキングアクション:インスペクションなしでトラフィックをブロック

ライセンス:すべて

ブロックアクションおよびリセット付きブロックアクションはトラフィックを拒否し、いかなる種類の追加のインスペクションも行われません。リセット付きブロックルールでは接続のリセットも行います。



復号化された HTTP トラフィックの場合、システムが Web 要求をブロックすると、デフォルトのブラウザまたはサーバのページを、接続が拒否されたことを説明するカスタムページでオーバーライドできます。システムではこのカスタムページを *HTTP 応答ページ*と呼んでいます。[ブロックされた URL のカスタム Web ページの表示 \(8-16 ページ\)](#)を参照してください。

ブロックされたネットワークトラフィックは、接続の開始時にのみログに記録できます。インラインで展開されたデバイスのみがトラフィックをブロックできることに注意してください。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。詳細については、[ブロックされた接続およびインタラクティブにブロックされた接続のログギングについて \(35-6 ページ\)](#)を参照してください。



注意

サービス妨害 (DoS) 攻撃の間にブロックされた TCP 接続をログギングすると、複数の同様のイベントによってシステムパフォーマンスに影響を受ける可能性があります。ブロックルールに対してログギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

インタラクティブブロッキングアクション: ユーザがWebサイトブロックをバイパスすることを許可する

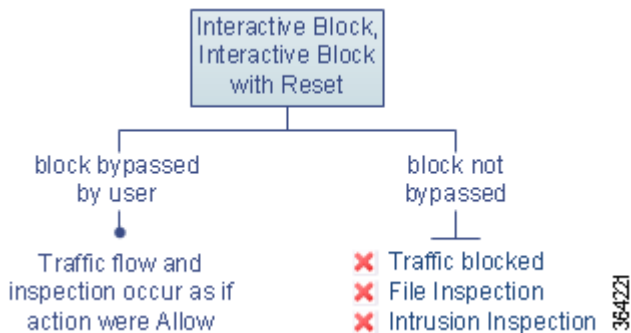
ライセンス: すべて

復号化された HTTP トラフィックの場合、インタラクティブブロックアクションおよびリセット付きインタラクティブブロックアクションを使用すると、ユーザはカスタマイズ可能な警告ページ (HTTP 応答ページと呼ばれます) をクリックスルーすることで、Web サイトのブロックをバイパスできます。リセット付きインタラクティブブロックルールでは接続のリセットも行います。

Web トラフィックを復号化する SSL インスペクションを設定し、そのトラフィックがインタラクティブブロックルールに一致する場合、システムは応答ページを暗号化し、再度暗号化された SSL 応答ストリームの最後にそのページを送信します。

インタラクティブにブロックされたすべてのトラフィックに対し、システムの処理、インスペクション、およびロギングは、ユーザがブロックをバイパスするかどうかによって異なります。

- 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、接続の開始のみをロギングできます。これらの接続開始イベントには、Interactive Block または Interactive Block with Reset アクションが付きます。
- ユーザがブロックをバイパスする場合は、ルールは許可ルールを模倣します。このため、一方のタイプのインタラクティブブロックルールをファイルおよび侵入ポリシーに関連付け、このユーザ許可されたトラフィックを検査できます。さらにシステムは、接続イベントの開始と終了の両方をログに記録できます。これらの接続イベントには Allow アクションが付きます。



許可アクション: トラフィックの許可および検査

ライセンス: すべて

許可アクションにより、一致するトラフィックの通過が許可されます。トラフィックを許可すると、関連付けられた侵入ポリシーまたはファイルポリシー(またはその両方)を使用して、暗号化されていないまたは復号化されたネットワークトラフィックをさらに検査してブロックすることができます。

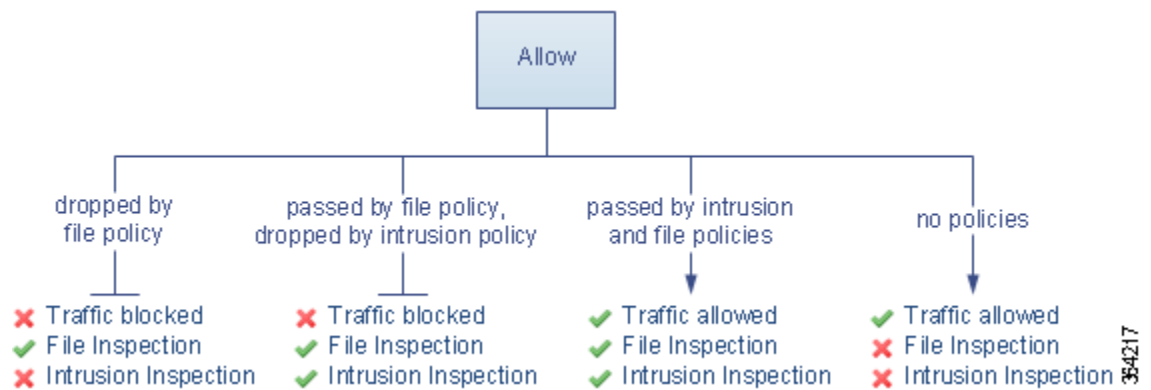
- Protectionライセンスを使用すると、侵入ポリシーを使用して、侵入検知および防御の設定に従ってネットワークトラフィックを分析し、必要に応じて、有害なパケットをドロップできます。
- また、Protectionライセンスを使用すると、ファイルポリシーを使用してファイル制御を実行できます。ファイル制御により、ユーザが特定のアプリケーションプロトコルを介して特定のタイプのファイルをアップロード(送信)またはダウンロード(受信)するのを検出およびブロックすることができます。

- マルウェアライセンスを使用すると、この場合もファイルポリシーを使用して、ネットワークベースの高度なマルウェア防御 (AMP) を実行できます。ネットワークベースの AMP は、マルウェアの有無についてファイルを検査し、必要に応じて検出されたマルウェアをブロックできます。

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方法については、[侵入ポリシーおよびファイルポリシーを使用したトラフィックの制御\(11-1 ページ\)](#)を参照してください。

下の図に、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(インタラクティブブロッキングアクション:ユーザが Web サイトブロックをバイパスすることを許可する(6-10 ページ)を参照)の条件)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 exploit 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。



許可されたネットワークトラフィックは、接続の開始および終了の両方でログに記録することができます。

ルールへのコメントの追加

ライセンス:すべて

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、ルールの変更日と変更理由を記したり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。

コメントをルールに追加する方法:

- ステップ 1** アクセスコントロールルールエディタで、[Comments]タブを選択します。
[Comments] ページが表示されます。
- ステップ 2** [New Comment]をクリックします。
[New Comment] ポップアップウィンドウが表示されます。
- ステップ 3** コメントを入力し、[OK]をクリックします。
コメントが保存されます。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** ルールを保存するか、編集を続けます。

ポリシー内のアクセスコントロールルールの管理

ライセンス:すべて

次の図に示すアクセスコントロールポリシーエディタの [Rules] タブでは、ポリシー内のアクセスコントロールルールを追加、編集、検索、移動、有効化、無効化、削除、または管理できます。






#	Name	So Zo	De Zo	So Ne	De Ne	Us	Ap	Sr	De	UR	Action	Icons
Administrator Rules <i>This category is empty</i>												
Standard Rules <i>This category is empty</i>												
MyCompany Rules												
1	IPS/Malware & Logging	any	any	any	any	any	any	any	any	any	Allow	Icons
Root Rules <i>This category is empty</i>												

各ルールで、ポリシーエディタには、ルールの名前、条件の概要、ルールアクション、および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を示すアイコンが表示されます。その他のアイコンは、次の表で説明するように、コメント、警告、エラー、およびその他の重要な情報を表します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。

表 6-2 アクセスコントロールポリシーエディタについて

アイコン	説明	操作
	侵入インスペクション	ルールのインスペクション オプションを編集するには、アクティブな(黄色)インスペクションアイコンをクリックします。 侵入ポリシーおよびファイルポリシーを使用したトラフィックの制御(11-1 ページ) を参照してください。アイコンが非アクティブ(白)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。
	ファイルおよびマルウェアのインスペクション	

表 6-2 アクセスコントロールポリシーエディタについて(続き)

アイコン	説明	操作
	ログイン	ルールのログイン オプションを編集するには、アクティブな(青色)ログイン アイコンをクリックします。 アクセスコントロールの処理に基づく接続のログイン(35-10 ページ) を参照してください。アイコンが非アクティブ(白)の場合、接続ログインがそのルールで無効になっています。
	コメント	ルールにコメントを追加するには、コメント列の数字をクリックします。 ルールへのコメントの追加(6-11 ページ) を参照してください。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。
	警告	アクセスコントロールポリシーエディタで、ポリシーのすべての警告を表示するポップアップ ウィンドウを表示するには、 [Show Warnings] をクリックします。 アクセスコントロールポリシーとルールのトラブルシューティング(4-13 ページ) を参照してください。
	エラー	
	情報	

アクセスコントロールルールの管理については、以下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\(6-3 ページ\)](#)
- [アクセスコントロールルールの検索\(6-13 ページ\)](#)
- [ルールのイネーブル化とディセーブル化\(6-14 ページ\)](#)
- [ルールの位置またはカテゴリの変更\(6-14 ページ\)](#)

アクセスコントロールルールの検索

ライセンス:すべて

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、アクセスコントロールルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ(ゾーン、ネットワーク、アプリケーションなど)ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループオブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、100Bao という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの **[Applications]** カラムが強調表示されます。100Bao という名前のルールもある場合は、**[Name]** カラムと **[Applications]** カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

ルールの検索方法:

-
- ステップ 1** 検索するポリシーのアクセスコントロールポリシーエディタで、[Search Rules]プロンプトをクリックして、検索文字列を入力し、Enter を押します。検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。
- 一致する値を含むルールのカラムが強調表示されます。表示されている(最初の)一致は、他とは区別できるように強調表示されます。
- ステップ 2** 目的のルールを探すには次の操作が利用できます。
- 照合ルールの間を移動する場合は、次の一致アイコン(▼)または前の一致アイコン(▲)をクリックします。
 - ページを更新し、検索文字列および強調表示をクリアする場合は、クリアアイコン(✕)をクリックします。
-

ルールのイネーブル化とディセーブル化

ライセンス:すべて

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。ルールを無効にすると、システムはネットワークトラフィックの評価に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。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。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。[アクセスコントロールルールの作成および編集\(6-3 ページ\)](#)を参照してください。

アクセスコントロールルールの状態を変更するには、次の手順を実行します。

-
- ステップ 1** 有効化または無効化するルールを含むポリシーの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て、ルールの状態を選択します。
- アクティブでないルールを有効にするには、[State] > [Enable]を選択します。
 - アクティブなルールを無効にするには、[State] > [Disable]を選択します。
- ステップ 2** [Store FirePOWER Changes]をクリックして、ポリシーを保存します。
- 変更を反映させるには、アクセスコントロールポリシーを適用する必要があります([設定変更の展開\(4-12 ページ\)](#)を参照してください)。
-

ルールの位置またはカテゴリの変更

ライセンス:すべて

アクセスコントロールルールを整理しやすくするために、すべてのアクセスコントロールポリシーにはシステムによって提供された3つのルールカテゴリ(管理者ルール、標準ルール、ルール)があります。これらのカテゴリは移動、削除、名前変更することはできませんが、カスタムカテゴリを作成することができます。

詳細については、以下を参照してください。

- [ルールの移動\(6-15 ページ\)](#)
- [新しいルール カテゴリの追加\(6-15 ページ\)](#)

ルールの移動

ライセンス:すべて

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、ルールのブリエンプションを回避できます。

次の手順では、アクセスコントロールポリシーエディタを使用して1つ以上のルールを同時に移動する方法について説明します。また、ルールエディタを使用して個々のアクセスコントロールルールを移動することもできます。[アクセスコントロールルールの作成および編集\(6-3 ページ\)](#)を参照してください。

規則を移動するには、次の手順を実行します。

-
- ステップ 1** 移動するルールを含むポリシーのアクセスコントロールポリシーエディタで、各ルールの空白領域をクリックしてルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。
- 選択したルールは強調表示されます。
- ステップ 2** ルールを移動します。カットアンドペーストおよびドラッグアンドドロップを使用することもできます。
- 新しい場所にルールをカットアンドペーストするには、選択したルールを右クリックし、[Cut]を選択します。次に、カットしたルールをペーストする場所の隣のルールの空白領域を右クリックし、[Paste above]または [Paste below]を選択します。2つの異なるアクセスコントロールポリシー間ではアクセスコントロールルールをコピーアンドペーストできないことに注意してください。
- ステップ 3** [Store FirePOWER Changes]をクリックして、ポリシーを保存します。
- 変更を反映させるには、アクセスコントロールポリシーを適用する必要があります([設定変更の展開\(4-12 ページ\)](#)を参照してください)。
-

新しいルール カテゴリの追加

ライセンス:すべて

アクセスコントロールルールを整理しやすくするために、すべてのアクセスコントロールポリシーにはシステムによって提供された3つのルールカテゴリ(管理者ルール、標準ルール、ルートルール)があります。これらのカテゴリは移動、削除、名前変更することはできませんが、標準ルールとルートルール間でカスタムカテゴリを作成することができます。

カスタムカテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

新しいカテゴリを追加するには、次の手順に従います。

-
- ステップ 1** ルールカテゴリを追加するポリシーのアクセスコントロールポリシーエディタで、[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、[Insert new category]を選択することもできます。

[Add Category] ポップアップ ウィンドウが表示されます。

ステップ 2 [Name]に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

ステップ 3 次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、最初の [Insert] ドロップダウンリストから [above Category] を選択した後、2 番目のドロップダウンリストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウンリストから [below rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- 既存のルールの上にルールを配置する場合は、ドロップダウンリストから [above rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4 [OK] をクリックします。

カテゴリが追加されます。名前を編集するには、カスタム カテゴリの横にある編集アイコン (✎) をクリックします。カテゴリを削除するには、削除アイコン (🗑) をクリックします。削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5 [Store FirePOWER Changes] をクリックして、ポリシーを保存します。
