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

侵入ポリシーとファイルポリシーは連携し、トラフィックがその宛先に許可される前の最後の防御ラインとして機能します。

- **侵入ポリシー**は、システムの侵入防御機能を制御します。ネットワーク分析ポリシーと侵入ポリシーについて を参照してください。
- **ファイル ポリシー**は、システムのネットワークベースのファイル制御および高度なマルウェア防御（AMP）機能を制御します。ファイル ポリシーの概要と作成 を参照してください。

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（ブロッキング）、SSL インスペクションベースの決定、およびトラフィックの復号化と前処理は、ネットワークトラフィックが侵入、禁止されたファイル、およびマルウェアの有無について検査される前に行われます。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。

侵入防御および AMP では、次の表で説明されている特定のライセンス機能を有効にする必要があります。

表 *1*:侵入インスペクションおよびファイル インスペクションのライセンス要件

機能	説明	License
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection
ファイル制御	ファイルタイプの伝送を検出し、任意でブロックします	Protection

機能	説明	License
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、追跡し、任意でブロックします	Malware

侵入、禁止されたファイル、およびマルウェアの有無についてトラフィックを検査する詳細については、以下を参照してください。

- 許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション （2 ページ）
- 侵入防御パフォーマンスの調整 （7 ページ）
- 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（20 ページ）

許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション

ライセンス：Protection または Malware

侵入ポリシーおよびファイル ポリシーは、トラフィックがその宛先に許可される前の最後の防衛ラインとして、システムの侵入防御、ファイル制御、およびAMP機能を制御します。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、SSL インスペクションの決定（復号化を含む）、復号化および前処理、およびアクセス コントロール ルールの選択は、侵入およびファイルのインスペクションの**前に**発生します。

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。アクセス コントロール ルールの条件は単純または複雑のどちらにもできます。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。

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）することができます。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処理とインスペクションの決定

インタラクティブ ブロック ルールには、許可ルールと同じインスペクション オプションがあることに留意してください。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。詳細については、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を参照してください。

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。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。

上記のシナリオの詳細と、ファイルポリシーおよび侵入ポリシーをアクセス 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 アクションに関連付ける手順については、以下を参照してください。

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について

ライセンス：Protection または Malware

（注） 侵入防御のデフォルト アクションによって許可されたトラフィックは、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

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。

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、システムは侵入の有無についてファイル 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。

（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。

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 の検査およびブロックも行います。

- 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 クラウド ルックアップ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 ファイルの性質を持つ 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。

AMP またはファイル制御を実行するアクセス コントロール ルールの設定

ライセンス：Protection または Malware

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。アクセス コントロール ルールにファイル ポリシーを関連付けた後、アクセス コントロール ルール エディタの [Logging] タブで [Log Files] チェックボックスをオフにします。詳細については、許可された接続のファイルおよびマルウェア イベント ロギングの無効化を参照してください。

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関係なく、関連付けられた接続の終了をロギングします。「ファイル イベントとマルウェア イベントに関連付けられた接続（自動）」を参照してください。

アクセス コントロール ルールにファイル ポリシーを関連付けるには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 アクセス コントロール ルールを使用して AMP またはファイル制御を設定するアクセス 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 新しいルールを作成するか、または既存のルールを編集します。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

アクセス コントロール ルール エディタが表示されます。

ステップ 4 ルール アクションが [Allow]、[Interactive Block]、または [Interactive Block with reset] のいずれかに設定されていることを確認します。

ステップ 5 [Inspection] タブを選択します。

[Inspection] タブが表示されます。

ステップ 6 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 [File Policy] 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 [None] を選択します。

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。ファイル ポリシーの作成を参照してください。

ステップ 7 [Add] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入

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

ライセンス：Protection

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。

システムが侵入ポリシーを使用してトラフィックを評価する場合、関連付けられた変数セットが使用されます。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、デフォルトのセットにあるデフォルトの変数を変更します。を参照してください。事前定義されたデフォルト変数の最適化

異なる侵入ポリシー変数セットのペアを各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インスペクションを実行するのに必要なリソースを不足している場合は、アクセス コントロール ポリシーを適用できません。詳細については、パフォーマンスを向上させるためのルールの簡素化を参照してください。

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

シスコでは ASA FirePOWER モジュールで複数の侵入ポリシーを提供しています。システムによって提供される侵入ポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーでは、VRT は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が提供されます。

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これらの 2 つの侵入ポリシーは、基本ポリシーとして「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 [Drop When Inline] の設定です。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。詳細については、システムによって提供されるポリシーとカスタム ポリシーの比較を参照してください。

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 ルールで呼び出された侵入ポリシーは、侵入を検出すると、侵入イベントを生成します。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自動的にロギングします。「侵入に関連付けられた接続（自動）」を参照してください。

アクセス コントロール ルールに侵入ポリシーを関連付けるには、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。

[Access Control Policy] ページが表示されます。

ステップ 2　アクセス コントロール ルールを使用して侵入インスペクションを設定するアクセス 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 新しいルールを作成するか、または既存のルールを編集します。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

アクセス コントロール ルール エディタが表示されます。

ステップ 4 ルール アクションが [Allow]、[Interactive Block]、または [Interactive Block with reset] のいずれかに設定されていることを確認します。

ステップ 5 [Inspection] タブを選択します。

[Inspection] タブが表示されます。

ステップ 6 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 [None] を選択します。

カスタム侵入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。侵入ポリシーの編集を参照してください。

注意 シスコの担当者から指示された場合を除き、[Experimental Policy 1] を選択しないでください。シスコでは、試験用にこのポリシーを使用します。

ステップ 7 オプションで、侵入ポリシーに関連付けられている**変数セット**を変更します。

表示される編集アイコン（）をクリックして、変数セットを編集できます。変数セットの操作を参照してください。

ステップ 8 [Save] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入

侵入防御パフォーマンスの調整

ライセンス：Protection

Cisco では、侵入行為の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するための機能を提供しています。これらのパフォーマンス設定は、各アクセス コントロール ポリシーごとに設定し、その設定はその親のアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

侵入に関するパターン一致の制限

ライセンス：Protection

イベント キューで許可するパケット数を指定できます。また、ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。

イベント キューの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

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。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Pattern Matching Limits] タブを選択します。

ステップ 5 次のオプションを修正できます。

- [Maximum Pattern States to Analyze Per Packet] フィールドに、キューに含めるイベントの最大数の値を入力します。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットを検査するには、[Disable Content Checks on Traffic Subject to Future Reassembly] を選択します。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[Disable Content Checks on Traffic Subject to Future Reassembly] をオフにします。検査を無効にすると、ストリームの検査の処理オーバーヘッドが減少し、パフォーマンスが向上する場合があります。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入

侵入ルールの正規表現制限のオーバーライド

ライセンス：Protection

パケット ペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。デフォルトの制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

⚠

注意 非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザ以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

次の表に、デフォルトの制限をオーバーライドするように設定できるオプションを示します。

表 *2:* 正規表現の制約オプション

オプション	説明
Match Limit State	[Match Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[制限に合わせる（Match Limit）] に設定した値を使用する • [Unlimited] を選択して、無制限の数の試行を許可する • [カスタム（Custom）] を選択して、[制限に合わせる（Match Limit）] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
Match Limit	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。
Match Recursion Limit State	[Match Recursion Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [Default] を選択して、[Match Recursion Limit] に設定した値を使用する • [Unlimited] を選択して、無制限の数の再帰を許可する • [Custom] を選択して、[Match Recursion Limit] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [Match Recursion Limit] が意味を持つためには、[Match Limit] よりも小さい必要があることに注意してください。
Match Recursion Limit	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

PCRE オーバーライドの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。
[Access Control Policy] ページが表示されます。

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。
アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Regular Expression Limits] タブを選択します。

ステップ 5 表「正規表現の制約オプション」にあるオプションはすべて変更できます。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入

パケットごとに生成される侵入イベントの制限

ライセンス：Protection

ルール エンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザ インターフェイスに報告します。複数のイベントが発生した場合、ルール エンジンが 1 個のパケットまたはパケット ストリームに対して複数のイベントを記録するように選択できます。これらのイベントのロギングにより、報告されたイベントを超えて情報を収集することができます。このオプションを設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

次の表に、1 個のパケットまたはストリームに対して記録されるイベントの数を決定するために設定できるオプションを示します。

表 *3:* 侵入イベント ロギング制限のオプション

オプション	説明
Maximum Events Stored Per Packet	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
Maximum Events Logged Per Packet	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[Maximum Events Stored Per Packet] の値を超えてはいけません。

オプション	説明
Prioritize Event Logging By	イベントキュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザインターフェイスから報告されます。次の中から選択できます。 • [priority]：イベントの優先順位によってキュー内のイベントを並べ替えます。 • [content_length]：最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコーダ イベントおよびプリプロセッサ イベントよりも優先されます。

1 個のパケットまたはストリームに対して記録されるイベント数の設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

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。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Intrusion Event Logging Limits] タブを選択します。

ステップ 5 表「侵入イベント ロギング制限のオプション」の任意のオプションを変更できます。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入

パケットおよび侵入ルール遅延しきい値の設定

ライセンス：Protection

デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とともにセキュリティのバランスを保つことができます。

パケット遅延しきい値構成について

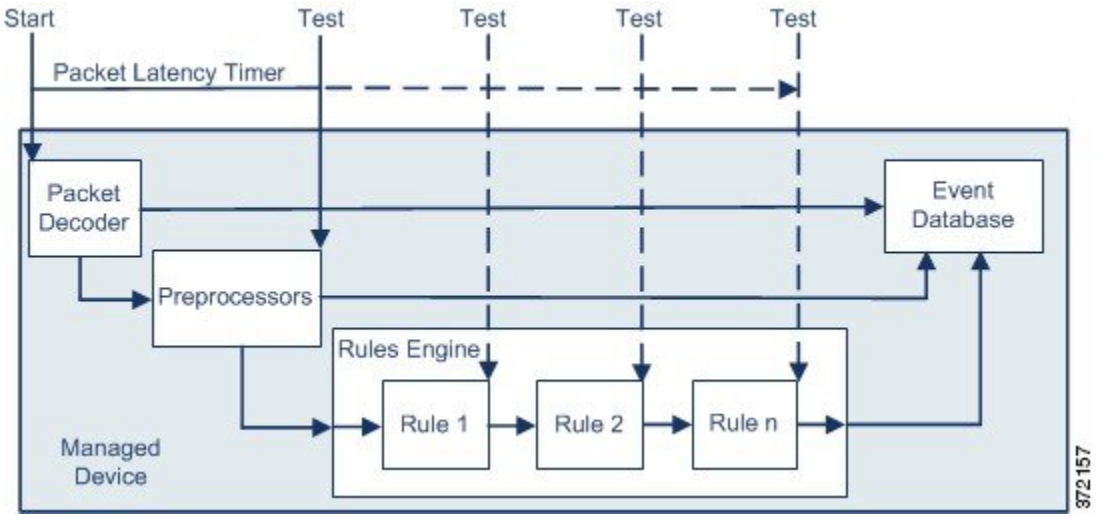
ライセンス：Protection

パケット遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、パケット遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミング テスト ポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間がいずれかのテスト ポイントでしきい値を超えると、パケット インスペクションは終了します。

ヒント パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケッ

ト処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

（注） パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

廃棄ルールの詳細については、を参照してください。 ルール状態の設定

パケット遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、過剰な処理時間を必要とするパケットのインスペクションを停止することで、インライン展開の遅延を減らすことができます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

パケット遅延しきい値の設定

ライセンス：Protection

次の表に、パケット遅延しきい値構成でユーザが設定できるオプションを示します。

表 *4:* パケット遅延しきい値構成オプション

オプション	説明
しきい値（マイクロ秒）	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、表「最小のパケット遅延しきい値設定」を参照してください。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了するイベントを生成できます。詳細については、「ルール状態の設定」を参照してください。

システム パフォーマンスおよびパケット遅延の測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 *5:* 最小のパケット遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	100
100 Mbps	250
5 Mbps	1000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

パケットインスペクションを不必要に中断することがないように、ネットワークの1パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

たとえば、表「最小のパケット遅延しきい値設定」では、1 ギガビット環境で 100 マイクロ秒の最小パケット遅延しきい値を推奨しています。この最小推奨値は、1 秒あたり平均 250,000 パケットを示すテストデータに基づいています。これは、1マイクロ秒あたり 0.25パケット、言い換えると 1 パケットあたり 4 マイクロ秒に相当します。25 倍すると推奨最小しきい値の 100 マイクロ秒が得られます。

パケット遅延しきい値の設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

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。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Latency-Based Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Packet Handling] タブを選択します。

ステップ 5 推奨される最小しきい値の設定については、表「最小のパケット遅延しきい値設定」を参照してください。

ステップ 6 [OK] をクリックします。

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保存して適用する必要があります。を参照してください。 設定変更の導入

ルール遅延しきい値構成について

ライセンス：Protection

ルール遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。ルールの遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間がルールの遅延しきい値を設定可能な回数を連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、ルール遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

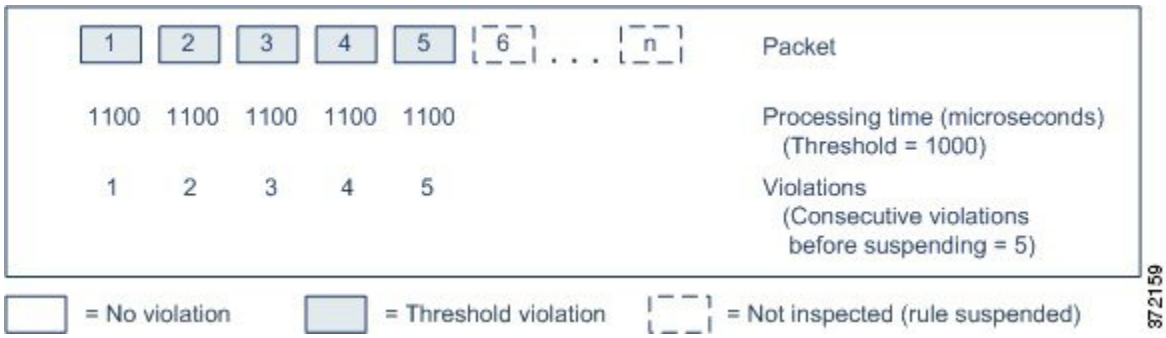
- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。

上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。廃棄ルールの詳細については、を参照してください。 ルール状態の設定

（注） パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット インスペクションを遅らせる場合

ルール遅延しきい値の設定

ライセンス：Protection

ルール遅延しきい値、一時停止されるルールの一時停止時間、ルールを一時停止する前に発生する必要がある連続したしきい値違反の回数を変更することができます。

ルールによるパケット処理時間が、[Consecutive Threshold Violations Before Suspending Rule] で指定された回数連続して [Threshold] を超えると、ルール遅延しきい値構成は [Suspension Time] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。詳細については、ルール状態の設定を参照してください。

次の表に、ルール遅延しきい値構成でユーザが設定できるオプションを示します。

表 *6:* ルール遅延しきい値構成のオプション

オプション	説明
しきい値	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、表「最小のルール遅延しきい値設定」を参照してください。
Consecutive Threshold Violations Before Suspending Rule	ルールが一時停止される前に、ルールによるパケットの検査時間が [Threshold] で設定された時間を超えることができる、連続した回数を指定します。
Suspension Time	ルールのグループを一時停止する秒数を指定します。

システム パフォーマンスの測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 *7:* 最小のルール遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	500
100 Mbps	1250
5 Mbps	5000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

ルールを不必要に一時停止することがないように、ネットワークの1パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

ルール遅延しきい値の設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

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。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Latency-Based Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Rule Handling] タブを選択します。

ステップ 5 表「ルール遅延しきい値構成のオプション」の任意のオプションを設定できます。

推奨される最小しきい値の設定については、表「最小のルール遅延しきい値設定」を参照してください。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入

侵入パフォーマンス統計情報のロギングの設定

ライセンス：Protection

デバイスがそのパフォーマンスを監視および報告する動作に関する基本的なパラメータを設定できます。これにより、次のオプションを設定することで、システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

[Sample time (seconds)] と [Minimum number of packets]

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

Troubleshooting Options：**Log Session/Protocol Distribution**

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

⚠

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

Troubleshooting Options：**Summary**

トラブルシューティングの電話中に、Snortプロセスのシャットダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[Log Session/Protocol Distribution] トラブルシューティング オプションも有効にする必要があります。

⚠

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

基本的なパフォーマンス統計情報パラメータの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

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。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（✎）をクリックし、表示されるポップアップ ウィンドウで [Performance Statistics] タブを選択します。

ステップ 5 前述のように、[Sample time] または [Minimum number of packets] を変更します。

ステップ 6 任意で、サポートによって求められた場合にのみ、[Troubleshoot Options] セクションを展開し、そのオプションを変更します。

ステップ 7 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の導入 を参照してください。

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

ライセンス：Protection または Malware

ファイル制御、またはマルウェアの検出あるいはブロッキングを行うためにファイルポリシーを使用する場合は、次の表にリストするオプションを設定できます。ファイルサイズを増やすと、システムのパフォーマンスに影響を与える可能性があることに注意してください。

表 *8*:アクセス コントロール ファイルおよびマルウェア検出の詳細オプション

フィールド	説明	デフォルト値	範囲	注意
Limit the number of bytes inspected when doing file type detection	ファイルタイプを検出するときに検査するバイト数を指定します。	1460 バイト、または TCP パケットの最大セグメント サイズ	0 ～ 4294967295（4 GB）	制限を取り除くには、0 に設定します。 ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
Do not calculate SHA-256 hash values for files larger than (in bytes)	システムが一定のサイズを超えるファイルを保管すること、ファイルで Collective Security Intelligence クラウドルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	10485760（10MB）	0 ～ 4294967295（4 GB）	制限を取り除くには、0 に設定します。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	マルウェア クラウドルックアップの実行中に、システムが [Block Malware] ルールに一致し、性質がキャッシュに入れられていないファイルを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	2 秒	0 ～ 30 秒	このオプションは最大 30 秒に設定できますが、デフォルト値を使用して、接続の障害によってトラフィックがブロックされないようにすることを推奨します。サポートに連絡することなく、このオプションを 0 に設定しないでください。

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を設定するには、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。

[Access Control Policy] ページが表示されます。

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。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Files and Malware Settings] の横にある編集アイコン（）をクリックします。

[Files and Malware Settings] ポップアップ ウィンドウが表示されます。

ステップ 5 表「アクセス コントロール ファイルおよびマルウェア検出の詳細オプション」の任意のオプションを設定できます。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入