侵入防御のパフォーマンスの調整

以下のトピックでは、侵入防御のパフォーマンスを調整する方法について説明します。

侵入防御のパフォーマンス チューニングについて

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。次の操作を実行できます。

- イベントキューで許可するパケット数を指定できます。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。
- 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。
- 複数のイベントが生成された場合にパケットまたはパケットストリームごとに複数のイベントをルールエンジンがログに記録するようにして、レポートされるイベント以外の情報も収集できます。
- 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セキュリティのバランスを保つことができます。

- デバイスがそのパフォーマンスをモニタ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。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。

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。

侵入防御パフォーマンスの調整のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入防御パフォーマンスの調整の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

侵入に関するパターン一致の制限

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、[詳細（Advanced）]（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[編集（Edit）]** > **[その他（More）]** > **[詳細設定（Advanced Settings）]**）をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある**[編集（Edit）]**（✎）をクリックします。

代わりに [表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、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 [パフォーマンス設定（Performance Settings）] ポップアップウィンドウ内の [パターン一致の制限（Pattern Matching Limits）] をクリックします。

ステップ 4 [パケットごとに分析するパターン状態の最大値（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。

ステップ 5 Snort 2 で、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、[今後の再構成の対象となるトラフィックでコンテンツチェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] チェックボックスをオンにします。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。

重要 Snort 3 では、[今後の再構成の対象となるトラフィックでコンテンツチェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] チェックボックスの設定は次のとおりです。

- オン：再構成前に TCP ペイロードを検出することを示します。これには、ストリームの再構成の前後のパケットのインスペクションが含まれます。このプロセスでは、より多くの処理オーバーヘッドが必要になり、パフォーマンスが低下する可能性があります。
- オフ：再構成後に TCP ペイロードを検出することを示します。

ステップ 6 [OK] をクリックします。

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。

正規表現による侵入ルールのオーバーライドの制限

デフォルトの正規表現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。

表 *1*: 正規表現の制約オプション

オプション	説明
検索結果の制限状態（Match Limit State）	[制限に合わせる（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 • [無制限（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
制限に合わせる（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。

オプション	説明
検索結果の再起制限状態（Match Recursion Limit State）	[再起制限に合わせる（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。 • [デフォルト（Default）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の再帰を許可する • [カスタム（Custom）] を選択して、[再起制限に合わせる（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 [再起制限に合わせる（Match Recursion Limit）] が意味を持つためには、[制限に合わせる（Match Limit）] よりも小さい必要があることに注意してください。
再起制限に合わせる（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。

関連トピック

概要：pcre キーワード

侵入ルールの正規表現制限のオーバーライド

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、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある**[編集（Edit）]**（✎）をクリックします。

代わりに [表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、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 [パフォーマンス設定（Performance Settings）] ポップアップウィンドウ内の [正規表現の制限（Regular Expression Limits）] をクリックします。

ステップ 4 正規表現による侵入ルールのオーバーライドの制限 （4 ページ）で説明するオプションを変更できます。

ステップ 5 [OK] をクリックします。

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。

パケットごとの侵入イベント生成の制限

侵入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。侵入イベント ロギングの制限を設定する場合、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。

表 *2:* 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
パケットごとに保存されるイベントの最大数（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。
パケットごとにログに記録され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、[パケットごとに保存されるイベントの最大数（Maximum Events Stored Per Packet）] 値を超えてはいけません。
イベント ロギングの順位決定の基準（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。

パケットごとに生成される侵入イベントの制限

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、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある**[編集（Edit）]**（✎）をクリックします。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、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 [パフォーマンス設定（Performance Settings）] ポップアップウィンドウ内の [侵入イベントのログ制限（Intrusion Event Logging Limits）] をクリックします。

ステップ 4 パケットごとの侵入イベント生成の制限 （6 ページ） に示したオプションを変更できます。

ステップ 5 [OK] をクリックします。

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。

パケットおよび侵入ルールの遅延しきい値構成

各アクセスコントロールポリシーには、しきい値を使用してパケットとルールの処理パフォーマンスを管理する、遅延ベースの設定があります。

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。

ルール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、処理時間が遅延しきい値ルールをある回数（設定可能）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。

遅延ベースのパフォーマンス設定

デフォルトでシステムが使用するパフォーマンス設定は、システムに導入された最新の侵入ルールの更新の遅延ベースのパフォーマンス設定です。

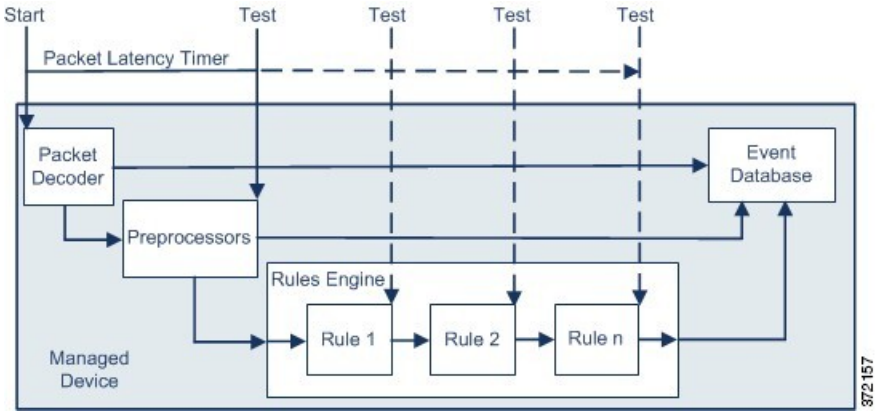
実際に適用される遅延の設定は、アクセス コントロール ポリシーと関連付けられているネットワーク分析ポリシー（NAP）のセキュリティ レベルによって異なります。通常、デフォルトの NAP ポリシーが関連付けられます。ただし、カスタム ネットワーク分析ルールが設定されている場合、ルールの中にデフォルトの NAP ポリシーより強力な NAP ポリシーを指定しているものがあれば、カスタム ルールの中で最もセキュアな NAP ポリシーが、遅延の設定のベースとなります。デフォルトの NAP ポリシーまたはカスタム ルールによってカスタム NAP ポリシーが呼び出された場合、評価で使用されるセキュリティ レベルは、それぞれのカスタム NAP ポリシーがベースとするシステム提供のベース ポリシーになります。

以上の説明は、有効なしきい値やネットワーク分析の設定が継承されるか、ポリシーに直接構成されるかにかかわらず当てはまります。

パケット遅延しきい値構成

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、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

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。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

処理時間が任意のテスト ポイントでしきい値を超えると、パケットの検査は停止します。

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。

パケット遅延のしきい値は、パッシブおよびインライン展開の両方でシステムのパフォーマンスを向上させ、インライン展開では過度の処理時間を必要とするパケットの検査を停止することにより遅延を低減できます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- 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構成の注意事項

デフォルトでは、パケット処理に関する遅延ベースのパフォーマンス設定は無効になっています。この設定を有効にすることもできます。ただし、シスコはしきい値設定のデフォルト値を変更しないことを推奨します。

下の情報は、カスタム値の指定を選択した場合にのみ適用されます。

表 *3:* 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）（Threshold (microseconds)）	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。

パケット遅延しきい値の有効化

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、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある**[編集（Edit）]**（）をクリックします。

代わりに[表示（View）]（）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。

ステップ 3 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップウィンドウで [パケット処理（Packet Handling）] をクリックします。

ステップ 4 [有効（Enabled）] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。

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。

パケット遅延しきい値の設定

デフォルトでは、パケット処理に関する遅延ベースのパフォーマンス設定は無効になっています。この設定を有効にすることもできます。ただし、シスコはしきい値設定のデフォルト値を変更しないことを推奨します。

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、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある**[編集（Edit）]**（）をクリックします。

システム（）**> [モニタリング（Monitoring）] > [統計（Statistics）]**

ステップ 3 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 4 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップウィンドウで [パケット処理（Packet Handling）] をクリックします。

デフォルトでは、[インストールされたルールの更新（Installed Rule Update）] が選択されます。このデフォルトを使用することを推奨します。

表示される値は、自動化された設定を反映しません。

ステップ 5 カスタム値を指定する場合は、次の点に注意してください。

- [有効（Enabled）] チェックボックスをオンにして、パケット遅延しきい値構成の注意事項（9 ページ）を参照して推奨される最小の [しきい値（Threshold）] 設定を確認します。
- パケット処理タブとルール処理タブの両方にカスタム値を指定する必要があります。

ステップ 6 [OK] をクリックします。

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。

ルール遅延しきい値構成

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、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

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。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。

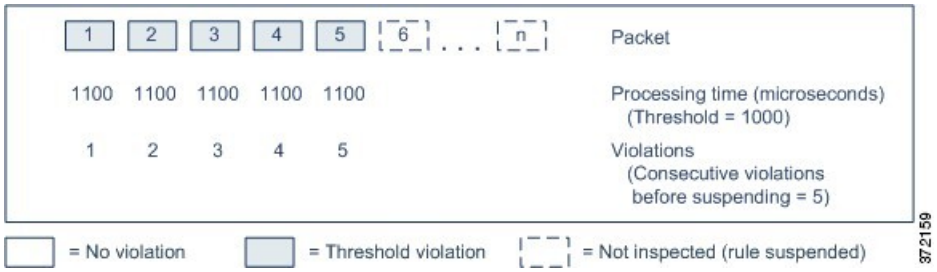
- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

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。

（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上のメリットは、以下のような場合にもたらされます。

- 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
- ユーザー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構成の注記

デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことを推奨します。

このトピックの情報は、カスタム値の指定を選択した場合にのみ適用されます。

ルールによるパケット処理時間が、[ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）] で指定された回数連続して [しきい値（Threshold）] を超えると、ルール遅延しきい値構成は [停止時間（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。侵入ルールの状態オプションを参照してください。

表 *4:* 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（Threshold）	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。
ルール停止前の連続しきい値違反（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 [しきい値（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。
停止時間（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。

ルール遅延しきい値の設定

デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことを推奨します。

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、[詳細（Advanced）] をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある**[編集（Edit）]**（）をクリックします。

代わりに[表示（View）]（）が表示される場合、設定は先祖ポリシーから継承されており、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 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップウィンドウで [ルール処理（Rule Handling）] をクリックします。

デフォルトでは、[インストールされたルールの更新（Installed Rule Update）] が選択されます。このデフォルトを使用することを推奨します。

表示される値は、自動化された設定を反映しません。

ステップ 4 カスタム値を指定する場合は、次の点に注意してください。

- ルール遅延しきい値構成の注記 （13 ページ）の任意のオプションを設定できます。
- パケット処理タブとルール処理タブの両方にカスタム値を指定する必要があります。

ステップ 5 [OK] をクリックします。

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

- イベントを生成するには、遅延ルール（134:1 と 134:2）を有効にします。詳細については、侵入ルールの状態オプションを参照してください。
- 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。

侵入パフォーマンス統計情報のロギング設定

[サンプル時間（秒）（Sample time (seconds)）] と [パケットの最小数（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。

⚠

注意 サンプル時間に非常に低い値（1 秒など）を設定すると、デバイスに大きな影響を与える可能性があります。デバイスに記録されたパフォーマンス統計情報がディスク容量の問題を引き起こし、デバイスの動作に影響を与える可能性があります。したがって、非常に低い値を設定しないことをお勧めします。

トラブルシューティング オプション：[ログ セッション/プロトコル分布（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 サポートによって指示された場合を除き、[ログセッション/プロトコル分布（Log Session/Protocol Distribution）] を有効にしないでください。

トラブルシューティング オプション：[概要（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、[ログ セッション/プロトコル分布（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 サポートから指示された場合を除き、[概要（Summary）] を有効にしないでください。

侵入パフォーマンス統計情報のロギングの設定

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 [詳細（Advanced）] をクリックし、[パフォーマンス設定（Performance Settings）] の横にある**[編集（Edit）]**（✎）をクリックします。

新しい UI で、パケットフロー行の最後にあるドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

代わりに[表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、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 2 表示されるポップアップウィンドウの [パフォーマンス統計情報（Performance Statistics）] をクリックします。

ステップ 3 侵入パフォーマンス統計情報のロギング設定 （14 ページ） での説明通り、[サンプル時間（Sample time）] または [パケットの最小数（Minimum number of packets）] を変更します。

注意 [サンプル時間（Sample time）] に非常に低い値（1 秒など）を設定すると、デバイスに大きな影響を与える可能性があります。デバイスに記録されたパフォーマンス統計情報がディスク容量の問題を引き起こし、デバイスの動作に影響を与える可能性があります。したがって、非常に低い値を設定しないことをお勧めします。

ステップ 4 任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション（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 5 [OK] 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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。