侵入イベント ロギングのグローバルな制限

システムが侵入イベントを記録して表示する回数を制限するしきい値を使用できます。侵入ポリシーの一部としてしきい値を設定すると、ルールに一致するトラフィックが指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、多数のイベントでいっぱいになることを回避できます。この機能を使用するには保護ライセンスが必要です。

イベント通知しきい値は、次の 2 種類の方法で設定できます。

- すべてのトラフィックに対するグローバルしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントが記録され表示される頻度を制限できます。詳細については、しきい値について（35-1 ページ）およびグローバルしきい値の設定（35-3 ページ）を参照してください。
- 侵入ポリシー設定での共有オブジェクトのルール、標準テキスト ルール、プリプロセッサ ルールごとにしきい値を設定できます。イベントしきい値の設定（32-26 ページ）を参照してください。

しきい値について

ライセンス：保護

デフォルトでは、侵入ポリシーごとに、グローバル ルールしきい値が含まれます。デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。このグローバルしきい値は、デフォルトですべての侵入ルールとプリプロセッサ ルールに適用されます。しきい値は侵入ポリシーの [詳細設定（Advanced Settings）] ページで無効にできることに注意してください。

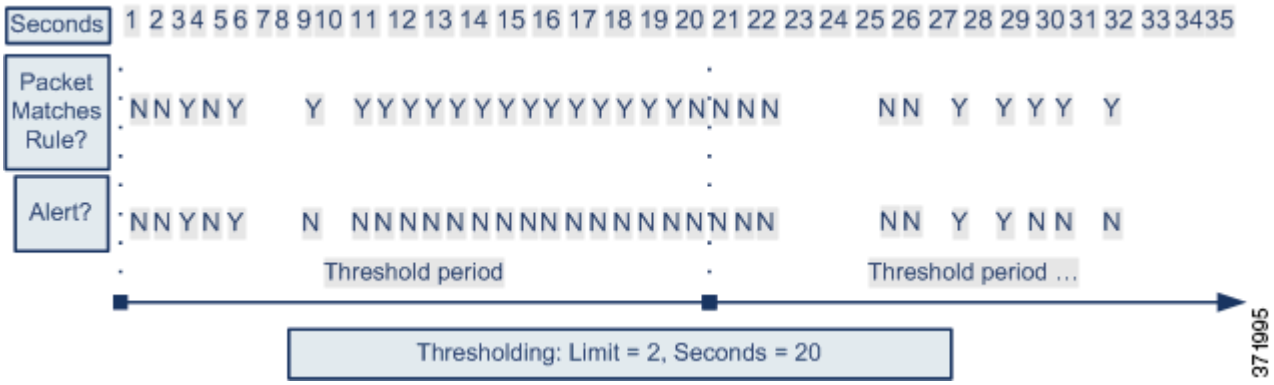
特定のルールで個々のしきい値を設定することにより、このしきい値を上書きすることもできます。たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。

ルール ベースのしきい値の設定の詳細については、イベントしきい値の設定（32-26 ページ）を参照してください。

ヒント 複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

次の図は、特定のルールに関して攻撃を受けている例を示します。グローバル制限しきい値では、各ルールのイベント生成が、20 秒あたり 2 つのイベントに制限されます。

期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の 2 つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



しきい値のオプションについて

ライセンス:保護

しきい値を使用して、期間内に特定数のイベントのみが生成されるように制限するか、イベントセットごとに 1 つのイベントが生成されるように制限することで、侵入イベントの生成を制限できます。グローバルしきい値を設定する際は、最初にしきい値のタイプを指定する必要があります。以下の表を参照してください。

表 35-1　しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定します。これにより、イベント インスタンスの数が送信元 IP アドレスと宛先 IP アドレスのどちらに基づいて計算されるかが決まります。最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 35-2　インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数（Count）	しきい値を満たすために必要な、トラッキング IP アドレスまたはアドレス範囲ごとの、指定された期間でのイベント インスタンスの数。
秒（Seconds）	カウントがリセットされるまでの秒数。しきい値タイプを [制限（Limit）] に、トラッキングを [送信元（Source）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 10 に設定した場合、特定の送信元ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

グローバルしきい値の設定

ライセンス：保護

一定の期間に各ルールによって生成されるイベントの数を管理するために、グローバルしきい値を設定できます。グローバルしきい値を設定すると、特定のしきい値を上書きしない各ルールでそのしきい値が適用されます。しきい値の設定の詳細については、しきい値について（35-1 ページ）を参照してください。

デフォルトでは、ユーザのシステムにグローバルしきい値が設定されます。デフォルト値は次のとおりです。

- タイプ（Type）：制限（Limit）
- 追跡対象（Track By）：宛先（Destination）
- カウント（Count）：1
- 秒（Seconds）：60

グローバルしきい値の設定方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

手順 4　[侵入ルールしきい値(Intrusion Rule Thresholds)] の [グローバル ルールのしきい値構成(Global Rule Thresholding)] が有効になっているかどうかに応じて、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[グローバル ルールのしきい値構成(Global Rule Thresholding)] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(24-1 ページ)を参照してください。

手順 5　[タイプ(Type)] オプション ボタンから、seconds 引数で指定された時間内に適用するしきい値のタイプを選択します。詳細については、しきい値設定オプションの表を参照してください。

- count 引数で指定された制限を超えるまで、ルールをトリガーとして使用したパケットごとにイベントを記録して表示する場合、[制限(Limit)] を選択します。
- ルールをトリガーとして使用し、count 引数で設定されたしきい値と同じかその倍数であるインスタンスを表すパケットごとに 1 つのイベントを記録して表示する場合、[しきい値(Threshold)] を選択します。
- count 引数によって指定された数のパケットがルールをトリガーとして使用した後に 1 つのイベントを記録して表示する場合、[両方(Both)] を選択します。

手順 6　[追跡対象(Track By)] ドロップダウンリストからトラッキング方法を選択します。

- 特定の送信元 IP アドレスからのトラフィックでルールの一致を識別するには、[送信元(Source)] を選択します。
- 特定の宛先 IP アドレスへのトラフィックでルールの一致を識別するには、[宛先(Destination)] を選択します。

手順 7　[カウント(Count)] フィールドで以下を実行します。

- [制限(Limit)] しきい値では、しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数を指定します。
- [しきい値(Threshold)] しきい値では、しきい値として使用するルールの一致回数を指定します。

手順 8　[秒(Seconds)] フィールドで以下を実行します。

- [制限(Limit)] しきい値では、攻撃を追跡する期間の秒数を指定します。
- [しきい値(Threshold)] しきい値では、カウントをリセットするまでの経過時間(秒数)を指定します。指定された秒数が経過する前であっても、[カウント(Count)] フィールドで示されている数のルールが一致すると、カウントはリセットされるのでご注意ください。

手順 9　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

グローバルしきい値の無効化

ライセンス:保護

デフォルトでは、グローバル制限しきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。デフォルトで特定のルールに関するイベントにしきい値を適用し、すべてのルールにしきい値を適用しない場合、最高位のポリシー階層でグローバルしきい値を無効にできます。

グローバルしきい値を無効にする方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [侵入(Intrusion)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

手順 3　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

手順 4　[侵入ルールしきい値(Intrusion Rule Thresholds)] で、[グローバル ルールのしきい値構成(Global Rule Thresholding)] を無効化します。

手順 5　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定(23-17 ページ)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。