



侵入イベント ログイングのグローバル制限

次のトピックでは、侵入イベント ログイングをグローバルに制限する方法について説明します。

- [グローバル ルールのしきい値の基本 \(1 ページ\)](#)
- [グローバル ルールしきい値オプション \(2 ページ\)](#)
- [グローバルなしきい値の設定 \(5 ページ\)](#)
- [グローバルしきい値の無効化 \(6 ページ\)](#)

グローバル ルールのしきい値の基本

グローバルルールのしきい値は、侵入ポリシーによってイベント ログイングの限界を設定します。すべてのトラフィックに対するグローバルルールの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ポリシーで記録および表示される頻度を制限できます。ポリシー内で共有オブジェクトのルール、標準テキストルール、またはプリプロセッサルールごとに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、上書きする特定のしきい値を指定していないポリシー内の各ルールでそのしきい値が適用されます。しきい値により、多数のイベントでいっぱいになることを回避できます。

すべての侵入ポリシーにはデフォルトのグローバルルールしきい値が含まれていて、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。このデフォルトのしきい値は、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。

次の操作を実行できます。

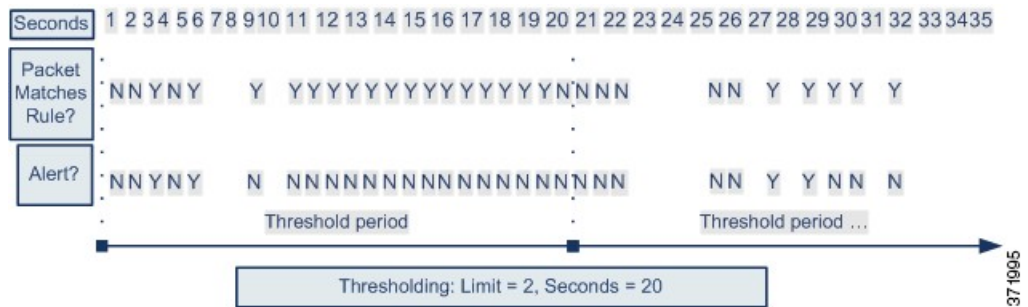
- グローバルしきい値の変更。
- グローバルしきい値の無効化。
- 特定のルールに個別のしきい値を設定して、グローバルしきい値の上書き。

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。



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。

次の図で、グローバルルールのしきい値がどのように機能するかを示します。この例では、特定のルールに対して攻撃が進行中です。グローバル制限しきい値は、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るように設定されています。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。



グローバルルールしきい値オプション

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。グローバルルールしきい値オプションのデフォルト値は次のとおりです。

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

これらのデフォルト値は次のように変更することができます。

表 1: しきい値のタイプ

| オプション | 説明 |
|-----------|--|
| Limit | <p>指定された数のパケット（カウント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。</p> <p>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。</p> |
| Threshold | <p>指定された数のパケット（カウント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。</p> <p>たとえば、タイプを [Threshold] に、[Count] を 10 に、[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 つのイベントを生成すると、[Seconds] と [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。</p> |

| オプション | 説明 |
|-------|---|
| Both | <p>指定された数（カウント）の packets 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。</p> <p>たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10 に設定した場合、イベント数は以下ようになります。</p> <ul style="list-style-type: none"> • 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回トリガーとして使用した場合、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回トリガーされると、しきい値が満たされ、以後のイベントは無視されるため）。 |

[追跡対象 (Track By)] オプションにより、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。

また、しきい値を定義するインスタンスの数と期間を次のように指定できます。

表 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 |
|-------|---|
| Count | <p>[制限 (Limit)] しきい値の場合は、しきい値を満たすために必要な、追跡する IP アドレスまたはアドレス範囲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。</p> <p>[しきい値 (Threshold)] しきい値の場合は、しきい値として使用するルールの一致回数。</p> |

| オプション | 説明 |
|-------------|---|
| 秒 (Seconds) | <p>[制限 (Limit)]しきい値の場合は、攻撃を追跡する期間の秒数。</p> <p>[しきい値 (Threshold)]しきい値の場合は、カウントをリセットするまでの経過時間 (秒数)。しきい値タイプを [Limit] に、トラッキングを [Source] に、 [Count] を 10 に、 [Seconds] を 10 に設定した場合、特定のソースポートで 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。</p> |

関連トピック

[グローバルなしきい値の設定 \(5 ページ\)](#)

[侵入イベントのしきい値](#)

グローバルなしきい値の設定

| 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数 | サポートされるドメイン数 | アクセス |
|-----------|------------|--------------|--------------|-----------------------|
| Threat | Protection | いずれか (Any) | いずれか (Any) | Admin/Intrusion Admin |

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 [Policies] > [Access Control] > [Intrusion] を選択します。

ステップ 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。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーションウィンドウで [詳細設定 (Advanced Settings)] をクリックします。

ステップ 4 [侵入ルールしきい値 (Intrusion Rule Thresholds)] で [グローバルルールしきい値 (Global Rule Thresholding)] が無効になっている場合は、 [有効化 (Enabled)] をクリックします。

ステップ 5 [グローバルルールしきい値 (Global Rule Thresholding)] の横にある編集アイコン (✎) をクリックします。

- ステップ 6** [タイプ (Type)] オプション ボタンを使用して、[秒 (Seconds)] フィールドで指定された時間内に適用するしきい値のタイプを指定します。
- ステップ 7** [追跡対象 (Track By)] オプション ボタンを使用して、追跡方法を指定します。
- ステップ 8** [カウント (Count)] フィールドに値を入力します。
- ステップ 9** [秒 (Seconds)] フィールドに値を入力します。
- ステップ 10** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

- [グローバル ルールしきい値オプション \(2 ページ\)](#)
- [レイヤでの侵入ルールの設定](#)
- [競合と変更：ネットワーク分析および侵入ポリシー](#)

グローバルしきい値の無効化

| 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数 | サポートされるドメイン数 | アクセス |
|------------|------------|--------------|--------------|-----------------------|
| Threat | Protection | いずれか (Any) | いずれか (Any) | Admin/Intrusion Admin |

デフォルトですべてのルールにしきい値を適用するのではなく、特定のルールに関するイベントにしきい値を適用する場合は、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。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 [Policies] > [Access Control] > [Intrusion] を選択します。

ステップ 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。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- ステップ3** ナビゲーション ウィンドウで [詳細設定 (Advanced Settings)] をクリックします。
- ステップ4** [侵入ルールしきい値 (Intrusion Rule Thresholds)] で、[グローバルルールしきい値 (Global Rule Thresholding)] の隣にある [無効 (Disabled)] をクリックします。
- ステップ5** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

[競合と変更：ネットワーク分析および侵入ポリシーレイヤでの侵入ルールの設定](#)

