侵入イベントロギングのグローバル制限

次のトピックでは、侵入イベントロギ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ライセンス要件 （4 ページ）
- グローバルしきい値の要件と前提条件 （4 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 ロギ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。

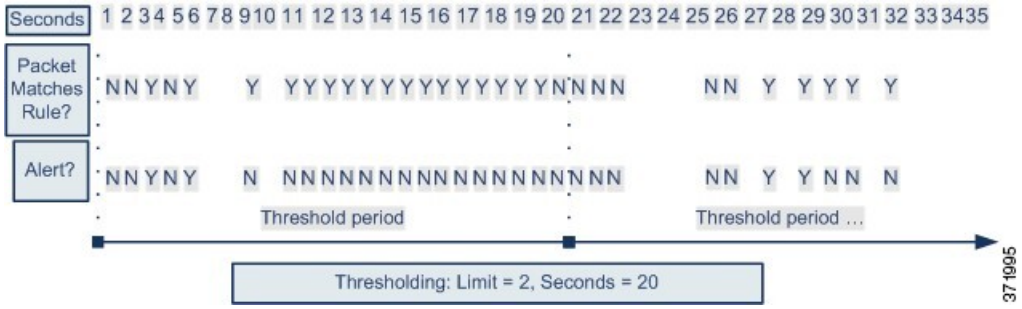
次の操作を実行できます。

- 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。

- 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

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
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。

オプション	説明
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（Both）	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）。 • 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）。

[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
カウント（Count）	[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。 [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。

オプション	説明
秒（Seconds）	[制限（Limit）] しきい値の場合は、攻撃を追跡する期間の秒数。 [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 [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。

関連トピック

グローバルなしきい値の設定 （5 ページ）
侵入イベントしきい値

グローバルなしきい値のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

グローバルしきい値の要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

グローバルなしきい値の設定

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[侵入（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 [Snort 2バージョン（Snort 2 Version）] 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 パネルで [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（Edit）]**（） をクリックします。

ステップ 6 [タイプ（Type）] 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）] を使用して、追跡方法を指定します。

ステップ 8 [数（Count）] フィールドに値を入力します。

ステップ 9 [秒数（Seconds）] フィールドに値を入力します。

ステップ 10 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（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：ネットワーク分析ポリシーと侵入ポリシー

グローバルしきい値の無効化

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。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[侵入（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 [Snort 2バージョン（Snort 2 Version）] 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 パネルで [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 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（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：ネットワーク分析ポリシーと侵入ポリシー
レイヤでの侵入ルールの設定

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。