レートフィルタ

レートフィルタの概要

タイプ	モジュール（基本）
使用方法	コンテキスト
インスタンス タイプ	単一
有効	`false`

レートベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することで低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レートベースの防御を使用し、そのルールの過剰な一致に応じて侵入のアクションを変更することができます。

`rate_filter` は、指定した間隔内にルールの一致が多すぎる場合にその状態を検出します。インライン展開された管理対象デバイス上でこの機能を使用して、指定された時刻のレートベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

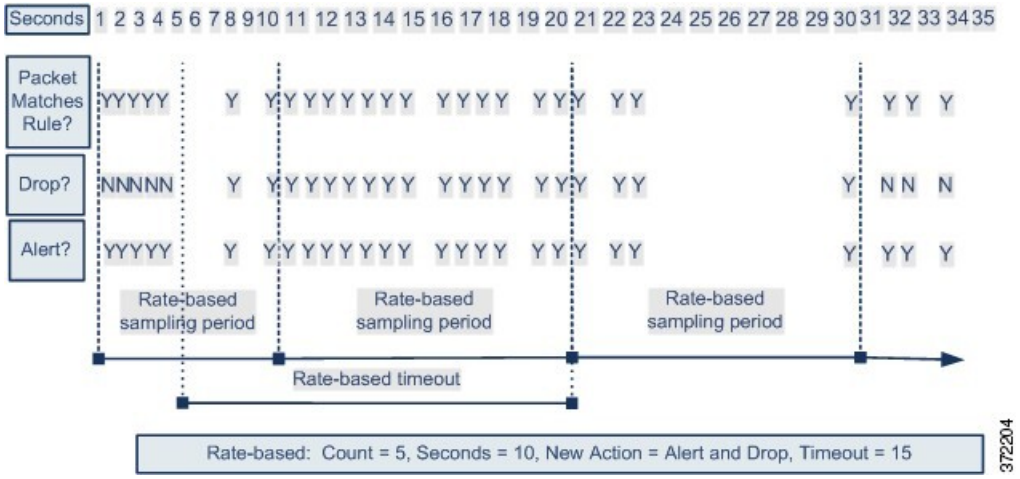
任意の侵入ルールに応じるように `rate_filter` は設定できますが、攻撃を検出して反応するようにするには、指定するルールを `rate_filter` で有効にする必要があります。たとえば、DDOS/SYN フラッド攻撃に対する防御を確立するには、ルール 135:1（TCP SYN を受信）を有効にして、ルール 135:1 の過剰なトリガーについて警告するように `rate_filter` を設定します。

レートベースの攻撃防止は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を

識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値を超えている場合は、新しいアクションが続行されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[イベントを生成する（Generate Events）] に戻ります。



同じルールだけでなく異なるルールにも複数のレートベースのフィルタを定義できます。複数のレートベースのフィルタが定義されている侵入ポリシーでは、ポリシーにリストされている最初のフィルタの優先度が最も高くなります。2 つのレートベースのフィルタアクションが競合している場合は、最初のレートベースのフィルタのアクションが実行されます。

`rate_filter`に設定した設定パラメータは、展開全体のすべてのトラフィックに適用されます。ただし、システムはそのシステムがモニタする一意の接続ごとにサンプリング期間内の一致の数に対して個別のカウンタを維持します。また、システムは、接続ごとにアクションに変更を適用します。

（注） レート ベース アクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。

レートフィルタのパラメータ

rate_filter[]

rate_filter 情報の配列を指定します。各 rate_filter には、トラフィックにレートベースの攻撃が含まれている場合にルールアクションを変更できる一連のフィールドが含まれています。

型：配列（オブジェクト）

例：

```
{
    "rate_filter": {
        "data": [
            {
                "apply_to": "[10.1.2.100, 10.1.2.101]",
                "count": 5,
                "gid": 135,
                "new_action": "alert",
                "seconds": 1,
                "sid": 1,
                "timeout": 5,
                "track": "by_src"
            }
        ],
        "enabled": true,
        "type": "singleton"
    }
}
```

rate_filter[].gid

照合するルールを識別するジェネレータ ID（GID）を指定します。

型：整数

有効な範囲：0 〜 4,294,967,295 (max32)

デフォルト値：1

rate_filter[].sid

照合するルールを識別する署名 ID（SID）を指定します。

型：整数

有効な範囲：0 〜 4,294,967,295 (max32)

デフォルト値：1

rate_filter[].track

送信元アドレスまたは接続先アドレスを照合するフィルタを指定します。

型：列挙体

有効な値は、次のとおりです。

- by_src：rate_filter[].gid と rate_filter[].sid によって指定されたルールに一致し、送信元アドレスが rate_filter[].apply_to と一致するトラフィックのみをフィルタ処理します。
- by_dst：gid と sid によって指定されたルールに一致し、宛先アドレスが rate_filter[].apply_to に一致するトラフィックのみをフィルタ処理します。
- by_rule：rate_filter[].gid と rate_filter[].sid によって指定されたルールに一致するすべてのトラフィックをフィルタ処理します。

デフォルト値：by_src

rate_filter[].count

代替アクション（rate_filter[].new_action）を適用する前に、サンプリング期間（rate_filter[].seconds）で許可するルール一致の数を指定します。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：1

rate_filter[].seconds

トラフィックを照合するサンプリング期間の秒数を指定します。rate_filter[].seconds は、一致の内部カウンタをゼロにリセットするまでに経過する時間を表します。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：1

rate_filter[].new_action

rate_filter[].seconds と rate_filter[].count で指定された制限を超えるトラフィック内で一致する応答で実行するアクションを指定します。

型：文字列

有効な値：文字列の alert、block、drop、log、pass、react、reject、rewrite のいずれかです。

デフォルト値：alert

rate_filter[].timeout

一致するトラフィックへの応答の rate_filter[].new_action で指定したアクションを実行する秒数を指定します。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：0

rate_filter[].apply_to

rate_filter[].track の値に応じて、トラフィックの送信元または接続先アドレスと照合するネットワークアドレスのリストを指定します。

型：文字列

有効な値：有効な IPv4 アドレス または CIDR 形式の IPv4 アドレスブロック。

デフォルト値：なし

レートフィルタのルール

rate_filter には、関連付けられたルールがありません。

侵入ルールに応答するように rate_filter を設定できます。ルールの rate_filter を有効にして、攻撃を検出して応答します。

レートフィルタの侵入ルールのオプション

rate_filter には、侵入ルールのオプションがありません。

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。